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

АНАЛИЗ И ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ КИБЕРБЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ
(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 «Анализ и показатели эффективности кибербезопасности предприятия» входит в программу бакалавриата «Кибербезопасность в экономике» по направлению 38.03.05 «Бизнес-информатика» и изучается в 6 семестре 3 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 3 разделов и 9 тем и направлена на изучение принципов анализа эффективности кибербезопасности предприятия.

Целью освоения дисциплины является изучение принципов анализа эффективности кибербезопасности предприятия, знакомство с нормативной базой, знакомство с основными показателями эффективности кибербезопасности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Анализ и показатели эффективности кибербезопасности предприятия» 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 «Анализ и показатели эффективности кибербезопасности предприятия» 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 «Анализ и показатели эффективности кибербезопасности предприятия».

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	Источники угроз кибербезопасности;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Seminar-Discussion on Business Informatics;
ПК-5	Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем	Экономическая безопасность; Источники угроз кибербезопасности; Технологии обеспечения кибербезопасности предприятий; Противодействие несанкционированным воздействиям в киберпространстве; Имитационное моделирование угроз экономической кибербезопасности; Бизнес-аналитика и методы принятия решений; Экономика "Умного города" и обеспечение безопасности ее функционирования;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Искусственный интеллект и кибербезопасность; Технологии распределенного реестра Blockchain; Финансовая безопасность;

* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО
** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Анализ и показатели эффективности кибербезопасности предприятия» 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)**
			6
Контактная работа, ак.ч.	*72*		*72*
Лекции (**ЛК**)	36		36
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	36		36
Самостоятельная работа обучающихся, ак.ч.	*45*		*45*
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	Подходы к оценке кибербезопасности предприятия	1.1	Организационные меры для обеспечения кибербезопасности	ЛК, СЗ
		1.2	Основные инструменты и приемы киберпреступников	ЛК, СЗ
		1.3	Современные тренды в кибербезопасности	ЛК, СЗ
Раздел 2	Анализ и показатели эффективности кибербезопасности по стандарту ГОСТ Р ИСО/МЭК 27004	2.1	Показатели и оценивание	ЛК, СЗ
		2.2	Мониторинг и оценка защищенности как процессы	ЛК, СЗ
		2.3	Примеры спецификаций по объектам мониторинга	ЛК, СЗ
Раздел 3	Знакомство с методами экспертных оценок	3.1	Задачи экспертного оценивания	ЛК, СЗ
		3.2	Способы измерения объектов	ЛК, СЗ
		3.3	Современные методы экспертного оценивания	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.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 или аналог. Дополнительное ПО: офисный пакет MS Office или LibreOffice.
Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и	Компьютер/ноутбук с доступом сети Интернет и электронно-

	консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или аналог. Дополнительное ПО: офисный пакет MS Office или LibreOffice.

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Мельников Сергей Юрьевич. Искусственный интеллект и кибербезопасность : учебное пособие / С.Ю. Мельников. - Электронные текстовые данные. - Москва : РУДН, 2023. - 72 с. : ил.
URL: https://lib.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=515838&idb=0

2. Модели безопасности компьютерных систем : учебное пособие / П.Н. Девянин. - М. : Академия, 2005. - 144 с. - (Высшее профессиональное образование). - ISBN 5-7695-2053-1 : 0.00.

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].

Дополнительная литература:

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт].

2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт].

3. 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.

4. Информационные системы в экономике и защита информации на предприятиях - участниках ВЭД : учебное пособие / А.В. Астахова. - Электронные текстовые данные. - Санкт-Петербург : Троицкий мост, 2014. - 214 с. : ил. - ISBN 978-5-4377-0040-2.

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 «Анализ и показатели эффективности кибербезопасности предприятия».

* - 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		Мельников Сергей 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.*