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

КИБЕРБЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

02.03.02 ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
(код и наименование направления подготовки/специальности)

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

ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
(наименование (профиль/специализация) ОП ВО)

2024 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Кибербезопасность предприятия» входит в программу бакалавриата «Фундаментальная информатика и информационные технологии» по направлению 02.03.02 «Фундаментальная информатика и информационные технологии» и изучается в 7 семестре 4 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 2 разделов и 8 тем и направлена на изучение подходов к обеспечению и оценки рисков кибербезопасности предприятия отрасли телекоммуникаций.

Целью освоения дисциплины является формирование у студентов профессиональных компетенций в области кибербезопасности предприятия отрасли телекоммуникаций на базе подходов Международного союза электросвязи по обеспечению и оценки рисков кибербезопасности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Кибербезопасность 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)
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Знает принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач; УК-1.2 Умеет анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности; УК-1.3 Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений;
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 анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ; УК-2.3 Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах;
ОПК-2	Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение, в том числе отечественного происхождения, для решения задач профессиональной деятельности	ОПК-2.1 Знает основные положения и концепции в области программирования, архитектуру языков программирования, знает основную терминологию, знаком с содержанием Единого Реестра Российских программ; ОПК-2.2 Умеет анализировать типовые языки программирования, составлять программы; ОПК-2.3 Имеет практический опыт решения задач анализа, интеграции различных типов программного обеспечения;
ОПК-5	Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной	ОПК-5.1 Знает методику установки и администрирования информационных систем и баз данных. Знаком с содержанием Единого реестра российских программ; ОПК-5.2 Умеет реализовывать техническое сопровождение информационных систем и баз данных; ОПК-5.3 Имеет практические навыки установки и

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	безопасности	инсталляции программных комплексов, применения основ сетевых технологий;
ПК-3	Способен осуществлять администрирование прикладного программного обеспечения, сетевой подсистемы и систем управления базами данных инфокоммуникационной системы организации	ПК-3.1 Знает основы архитектуры, устройства и функционирования информационно-вычислительных систем и сетевых подсистем инфокоммуникационной системы организации; методику установки и администрирования программных систем и сетевых подсистем инфокоммуникационной системы организации; ПК-3.2 Умеет настраивать и администрировать программные системы, сетевые подсистемы и базы данных инфокоммуникационной системы организации; ПК-3.3 Имеет практический опыт эксплуатации и администрирования программных систем, сетевых подсистем и баз данных инфокоммуникационной системы организации;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Кибербезопасность предприятия» относится к обязательной части 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 «Кибербезопасность 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*
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; Программная инженерия;	
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Философия; Математическое моделирование; Вычислительные системы, сети и телекоммуникации; Алгоритмы машинной графики и обработки изображений; Стохастический анализ беспроводных сетей; Программная инженерия; Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);	Технологическая (проектно-технологическая) практика; Научно-исследовательская работа; Преддипломная практика;
ОПК-2	Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение, в том числе отечественного	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Основы программирования;	Технологическая (проектно-технологическая) практика;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
	происхождения, для решения задач профессиональной деятельности	Технология программирования; Вычислительные методы; Математическое моделирование; Имитационное моделирование; Реляционные базы данных; Алгоритмы машинной графики и обработки изображений; Основы машинного обучения и нейронные сети; Теория автоматов и формальных языков; Стохастический анализ беспроводных сетей; Программная инженерия; Компьютерная алгебра; Архитектура компьютеров и операционные системы; Компьютерная геометрия;	
ОПК-5	Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	Реляционные базы данных; Программная инженерия; Архитектура компьютеров и операционные системы; Основы информационной безопасности;	Технологическая (проектно-технологическая) практика;
ПК-3	Способен осуществлять администрирование прикладного программного обеспечения, сетевой подсистемы и систем управления базами данных инфокоммуникационной системы организации	Сетевые технологии; Администрирование сетевых подсистем; Администрирование локальных сетей; Реляционные базы данных; Вычислительные системы, сети и телекоммуникации; Архитектура компьютеров и операционные системы; Основы информационной безопасности; Машинное обучение в телекоммуникациях; Обработка больших данных с использованием машинного обучения;	Технологическая (проектно-технологическая) практика; 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 «Кибербезопасность предприятия» 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)**
			7
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	Обеспечение кибербезопасности предприятия	1.1	Природа среды кибербезопасности предприятия. Основные методы защиты сетей связи предприятия	ЛК, СЗ
		1.2	Базовые принципы по обеспечению кибербезопасности предприятия	ЛК, СЗ
		1.3	Методы предотвращения кибератак на базе веб-сети в предприятии	ЛК, СЗ
		1.4	Процедура реагирования на инциденты кибербезопасности. Применение оперативной информации об угрозах	ЛК, СЗ
Раздел 2	Оценка рисков кибербезопасности предприятия	2.1	Использование структурированного представления информации об угрозах STIX	ЛК, СЗ
		2.2	Показатели риска в области кибербезопасности предприятия	ЛК, СЗ
		2.3	Оценка безопасности в сетях связи предприятия	ЛК, СЗ
		2.4	Улучшение восприятия клиентами показателей благонадежности веб-сайта предприятия	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
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
Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер,

	компьютерами с доступом в ЭИОС.	ПО для просмотра PDF, MS Teams

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Рекомендация МСЭ-Т X.1205 Обзор кибербезопасности https://www.itu.int/rec/T-REC-X.1205-200804-I

2. Рекомендация МСЭ-Т X.1207 Руководящие принципы решения проблемы риска проникновения шпионского ПО и потенциально нежелательного ПО, предназначенные для поставщиков услуг электросвязи https://www.itu.int/rec/T-REC-X.1207-200804-I/en

3. Рекомендация МСЭ-Т X.1211 Методы предотвращения атак на базе веб-сети https://www.itu.int/rec/T-REC-X.1211-201409-I/en

4. Рекомендация МСЭ-Т X.1216 Требования к сбору и сохранению доказательств инцидентов кибербезопасности https://www.itu.int/rec/T-REC-X.1216-202009-I/en

5. Рекомендация МСЭ-Т X.1217 Руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи https://www.itu.int/rec/T-REC-X.1217-202101-I/en

6. Рекомендация МСЭ-Т X.1215 Сценарии использования структурированного представления информации об угрозах https://www.itu.int/rec/T-REC-X.1215-201901-I/en

7. Рекомендация МСЭ-Т X.1208 Показатель риска в области кибербезопасности для укрепления доверия и безопасности при использовании электросвязи/информационнокоммуникационных технологий https://www.itu.int/rec/T-REC-X.1208-201401-I/en

8. Рекомендация МСЭ-Т X.1214 Методы оценки безопасности в сетях электросвязи/информационнокоммуникационных технологий https://www.itu.int/rec/T-REC-X.1214-201803-I/en

9. Рекомендация МСЭ-Т X.1212 Проектные решения для улучшенного восприятия конечным пользователем показателей благонадежности https://www.itu.int/rec/T-REC-X.1212-201703-I/en

Дополнительная 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: 26.04.2023). — Режим доступа: для авториз. пользователей.

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/

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

1. Курс лекций по дисциплине «Кибербезопасность предприятия».

* - 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 «Кибербезопасность предприятия» 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		Кочеткова Ирина Андреевна
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.*