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:

09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА
(код и наименование направления подготовки/специальности)

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

ПРИКЛАДНАЯ ИНФОРМАТИКА
(наименование (профиль/специализация) ОП ВО)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Кибербезопасность предприятия» входит в программу бакалавриата «Прикладная информатика» по направлению 09.03.03 «Прикладная информатика» 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 основ кибербезопасности предприятия.

Целью освоения дисциплины является формирование у студентов профессиональных компетенции в области основ кибербезопасности предприятия.

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-10	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-10.1 Знает основные понятия социально-экономических наук и правила принятия решений в различных областях жизнедеятельности; УК-10.2 Умеет обосновывать и применять основные положения и методы социально-экономических наук для принятия решений в различных областях жизнедеятельности; УК-10.3 Владеет методами для принятия экономических решений в различных областях жизнедеятельности;
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-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.1 Знает основы математики, физики, вычислительной техники и программирования; ОПК-1.2 Умеет решать стандартные профессиональные задачи с применением естественнонаучных и обще-инженерных знаний, методов математического анализа и моделирования; ОПК-1.3 Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности;
ОПК-2	Способен использовать современные информационные	ОПК-2.1 Знает современные информационные технологии и программные средства, в том числе отечественного

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	технологии и программные средства, в том числе, отечественного производства, при решении задач профессиональной деятельности	производства при решении задач профессиональной деятельности; ОПК-2.2 Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности; ОПК-2.3 Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности;
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ОПК-3.1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности;
ОПК-7	Способен разрабатывать алгоритмы и программы, пригодные для практического применения	ОПК-7.1 Знает основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий; ОПК-7.2 Умеет применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ; ОПК-7.3 Владеет навыками программирования, отладки и тестирования прототипов программно-технических комплексов;
ПК-5	Администрирование прикладного и системного программного обеспечения; управление программно-аппаратными средствами информационных служб	ПК-5.1 Знает основы архитектуры, устройства и функционирования информационно-вычислительных систем; методику установки и администрирования программных систем; ПК-5.2 Умеет реализовывать техническое сопровождение информационных систем; ПК-5.3 Имеет практический опыт эксплуатации и администрирования программных информационных систем;
ПК-6	Администрирование сетевой подсистемы инфокоммуникационной системы организации	ПК-6.1 Знает основы архитектуры, устройства и функционирования сетевых подсистем инфокоммуникационной системы организации; методику настройки и администрирования сетевых подсистем инфокоммуникационной системы организации; ПК-6.2 Умеет настраивать и администрировать сетевые подсистемы инфокоммуникационной системы организации; ПК-6.3 Имеет практический опыт эксплуатации и администрирования сетевых подсистем 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-10	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	Основы военной подготовки. Безопасность жизнедеятельности; Основы формальных методов описания бизнес-процессов; Введение в управление инфокоммуникациями; Основы экономики и менеджмента;	
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; Прикладное программное обеспечение: проектирование, управление проектом, разработка и документация; Основы теории массового обслуживания; Методы обучения и адаптации больших языковых моделей; Основы проектной деятельности;	
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Философия; Прикладное программное обеспечение: проектирование, управление проектом, разработка и документация; Машинное обучение в телекоммуникациях; Технологии искусственного интеллекта; Введение в программирование для мобильных платформ; Интеллектуальные методы разделения сетевых ресурсов; Теория автоматизации и управления; Введение в обучение с подкреплением; Java: базовые концепции и библиотеки классов; Имитационное моделирование; Методы искусственного интеллекта; Основы теории систем; Введение в специальность; Интеллектуальные системы;	Технологическая (проектно-технологическая) практика; Научно-исследовательская работа; Преддипломная практика;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
ОПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	Символьные методы математического анализа; Алгебра и аналитическая геометрия; Дискретная математика и математическая логика; Теория вероятностей и математическая статистика; Теория конечных графов; Символьные и численные методы интегрирования дифференциальных уравнений; Основы Web-технологий; Алгоритмы и структуры данных; Java: базовые концепции и библиотеки классов; Имитационное моделирование; Цифровая грамотность, основы программирования; Цифровая грамотность, технология программирования; Парадигмы программирования; Физика; Интеллектуальные системы; Химия и экология окружающей среды; Линейное и нелинейное программирование; Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);	Технологическая (проектно-технологическая) практика;
ОПК-2	Способен использовать современные информационные технологии и программные средства, в том числе, отечественного производства, при решении задач профессиональной деятельности	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Архитектура компьютеров и операционные системы; Реляционные базы данных; Основы Web-технологий; Сетевые технологии; Администрирование сетевых подсистем; Java: базовые концепции и библиотеки классов; Имитационное моделирование; Управление ИТ-сервисами и контентом; Цифровая грамотность, технология программирования; Парадигмы программирования; Основы информационной безопасности; Пакеты символьных вычислений в профессиональной деятельности; Интеллектуальные системы; Линейное и нелинейное программирование;	Технологическая (проектно-технологическая) практика;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Основы военной подготовки. Безопасность жизнедеятельности; Основы информационной безопасности; Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);	Технологическая (проектно-технологическая) практика;
ОПК-7	Способен разрабатывать алгоритмы и программы, пригодные для практического применения	Реляционные базы данных; Основы Web-технологий; Алгоритмы и структуры данных; Java: базовые концепции и библиотеки классов; Имитационное моделирование; Цифровая грамотность, основы программирования; Цифровая грамотность, технология программирования; Парадигмы программирования; Пакеты символьных вычислений в профессиональной деятельности; Интеллектуальные системы;	
ПК-6	Администрирование сетевой подсистемы инфокоммуникационной системы организации	Основы администрирования операционных систем; Сетевые технологии; Администрирование сетевых подсистем; Администрирование локальных сетей; Основы информационной безопасности;	
ПК-5	Администрирование прикладного и системного программного обеспечения; управление программно-аппаратными средствами информационных служб	Архитектура компьютеров и операционные системы; Основы администрирования операционных систем; Администрирование сетевых подсистем; Прикладное программное обеспечение: проектирование, управление проектом, разработка и документация; Управление ИТ-сервисами и контентом; Основы информационной безопасности;	

* - 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**)	36		36
Практические/семинарские занятия (**СЗ**)	0		0
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	Задачи обеспечения кибербезопасности предприятия	1.1	Среда кибербезопасности предприятия. Показатели риска и принципы по обеспечению кибербезопасности	ЛК, ЛР, СЗ
		1.2	Реагирование на инциденты кибербезопасности. Применение оперативной информации об угрозах. Структурированное представление информации об угрозах	ЛК, ЛР, СЗ
		1.3	Моделирование процедуры захвата и защиты базы данных предприятия	ЛК, ЛР, СЗ
Раздел 2	Кибербезопасность сети связи и веб-сайта предприятия	2.1	Оценка безопасности и методы защиты сети связи предприятия	ЛК, ЛР, СЗ
		2.2	Моделирование процедуры захвата и защиты контроллера домена предприятия	ЛК, ЛР, СЗ
		2.3	Подходы к предотвращению кибератак на базе веб-сети в предприятии	ЛК, ЛР, СЗ
		2.4	Улучшение восприятия клиентами показателей благонадежности веб-сайта предприятия	ЛК, ЛР, СЗ
		2.5	Моделирование процедуры захвата и защиты веб-сайта / корпоративного портала предприятия	ЛК, ЛР

* - 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.	
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве 22 шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, киберполигон Ampire
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, киберполигон Ampire

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Грушо Александр Александрович. Кибербезопасность предприятия : учебное пособие / А. А. Грушо, Е. Е. Тимонина. - Электронные текстовые данные . - Москва : РУДН, 2023. - 78 с. : ил.
URL: https://mega.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=510195&idb=0

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

3. 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

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

5. 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

6. 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

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

8. 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

9. 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

10. 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. Грушо Александр Александрович. Защита сетей и кибербезопасность : учебное пособие / А. А. Грушо, Е. Е. Тимонина, В. А. Бесчастный. - Электронные текстовые данные. - Москва : РУДН, 2023. - 88 с. : ил.
URL: https://mega.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=515837&idb=0

2. Ботвинко Анатолий Юрьевич. Технологии обеспечения кибербезопасности предприятий : учебное пособие / А. Ю. Ботвинко. - Москва : РУДН, 2023. - 95 с. : ил.

3. Ботвинко Анатолий Юрьевич. Источники угроз кибербезопасности : учебное пособие / А. Ю. Ботвинко. - Электронные текстовые данные. - Москва : РУДН, 2024. - 83 с. : ил.
URL: https://mega.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=516955&idb=0

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

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 «Кибербезопасность 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		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 математического моделирования и искусственного интеллекта		Малых Михаил Дмитриевич
Должность, БУП	*Подпись*	*Фамилия И.О.*