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

Защита сетей и кибербезопасность

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки:

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)

2023 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Защита сетей и кибербезопасность» является введение учащихся в предметную область современных методов защиты сетей и обеспечения кибербезопасности в бизнес-информатике. Для достижения поставленной цели выделяются задачи курса: освоение современных методов обеспечения защиты сетей и кибербезопасности предприятия, знакомство слушателей с основами анализа защиты сетей кибербезопасности и выводами, содержанием категорий, используемых в других дисциплинах, связанных с информационными технологиями.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Защита сетей и кибербезопасность» направлено на формирование у обучающихся следующих компетенций (части компетенций): ПК-3; ПК-4; ПК-5.

Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)

Шифр	**Компетенция**	**Индикаторы достижения компетенции** (в рамках данной дисциплины)
ПК-3	Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-3.1. Знает основы архитектуры, устройства и функционирования информационно-вычислительных систем и сетевых подсистем инфокоммуникационной системы организации; основы современных операционных систем; сетевые протоколы
		ПК-3.2. Знает основы программирования; современные объектно-ориентированные языки программирования; современные структурные языки программирования; языки современных бизнес-приложений
		ПК-3.3. Умеет кодировать на языках программирования
		ПК-3.4. Владеет навыками программирования для решения задач профессиональной деятельности
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	Способен решать задачи управления кибербезопасностью предприятий и иных	ПК-5.1. Знает методы организации управления кибербезопасностью предприятий и иных экономических систем
		ПК-5.2. Знает основы нормативно-правового

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	экономических систем	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 навыками 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 «Защита сетей и кибербезопасность» относится к части, формируемой участниками образовательных отношений, блока Б1 ОП ВО.

В рамках ОП ВО обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Защита сетей и кибербезопасность».

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики[1]
ПК-3	Способность выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	Архитектура компьютеров и операционные системы Основы программирования Технология программирования Компьютерный практикум Основы информатики и кибернетики Вычислительные системы, сети и телекоммуникации Основы информационной	Кибербезопасность предприятия, Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности) Преддипломная практика

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

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики
		безопасности Основы машинного обучения Основы анализа данных в машинном обучении	
ПК-4	Способность принимать обоснованные управленческие решения в своей профессиональной деятельности	Архитектура предприятия, ИТ-инфраструктура предприятия, Моделирование бизнес-процессов, Электронный бизнес, Рынки ИКТ и организация продаж, Технологии обеспечения кибербезопасности предприятий	Кибербезопасность предприятия, Искусственный интеллект и кибербезопасность, Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности), Преддипломная практика
ПК-5	Способность решать задачи управления кибербезопасностью предприятий и иных экономических систем	Цифровая трансформация глобальной экономики Международные платежные системы Дизайн мышление Экономическая безопасность в современных условиях Теневая экономика Киберполитика в международных экономических отношениях Мировая экономика Искусственный интеллект в бизнесе Финансовая безопасность Инновации в бизнесе Источники угроз кибербезопасности Технологии обеспечения кибербезопасности предприятий Противодействие несанкционированным воздействиям в киберпространстве	Кибербезопасность предприятия, Искусственный интеллект и кибербезопасность, Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности), Преддипломная практика

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Защита сетей и кибербезопасность» составляет 3 зачетные единицы.

Таблица 4.1. Виды учебной работы по периодам освоения ОП ВО

Вид учебной работы		**ВСЕГО,** ак.ч.	**Семестр(-ы)**
			6
Контактная работа, ак.ч.		*54*	*54*
в том числе:			
Лекции (**ЛК**)		18	18
Лабораторные работы (**ЛР**)		-	-
Практические/семинарские занятия (**СЗ**)		36	36
Самостоятельная работа обучающихся, ак.ч.		*54*	*54*
Контроль (экзамен/зачет с оценкой), ак.ч.		-	-
Общая трудоемкость дисциплины	ак.ч.	**108**	**108**
	зач.ед.	**3**	**3**

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы

Наименование раздела дисциплины	**Содержание раздела (темы)**	**Вид учебной работы**[2]
Раздел 1. Обзор сетевой инфраструктуры.	Тема 1.1. Сети, каналы, сетевые протоколы. Сетевое оборудование. Локальные сети предприятия. Семиуровневая модель описания сетевого взаимодействия.	ЛК, СЗ
	Тема 1.2. Глобальные сети. Социальные сети. Использование сетей в бизнес процессах.	ЛК, СЗ
	Тема 1.3. Участие персонала в социальных сетях. Инструменты воздействия на персонал.	ЛК, СЗ
Раздел 2. Сетевые угрозы. Вредоносные воздействия через сети.	Тема 2.1. 2.1 Вредоносный код (ВК). Угрозы, реализуемые ВК. Распространение ВК через сеть.	ЛК, СЗ
	Тема 2.2. Атаки на обслуживание.	ЛК, СЗ
	Тема 2.3. Бот сети. Сбор информации через сети.	ЛК, СЗ
Раздел 3. Архитектуры сетевой безопасности.	Тема 3.1.Архитектура безопасности семиуровневой модели. ИСО 7498 часть 2.	ЛК, СЗ
	Тема 3.2. Архитектура безопасности сетей в стеке TCP/IP. Протокол IPsec.	ЛК, СЗ
	Тема 3.3. Протоколы сетевой аутентификации. VPN. Инфраструктура открытых ключей.	ЛК, СЗ
Раздел 4. Механизмы защиты предприятия от сетевых атак.	Тема 4.1. 4.1 Системы обнаружения вторжений. IDS, SIEM	ЛК, СЗ
	Тема 4.2. Межсетевые экраны.	ЛК, СЗ
	Тема 4.3. Антивирусы. Демилитаризованная зона. DMZ.	ЛК, СЗ
	Тема 4.4. Прокси серверы.	ЛК, СЗ

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. 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. Дополнительное ПО: офисный пакет MS Office или LibreOffice.
Для самостоятельной работы обучающихся	Аудитория 210 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. Дополнительное ПО: офисный пакет MS Office или LibreOffice.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. 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]. — URL: https://urait.ru/bcode/490277

2. 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. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019

Дополнительная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490278
2. Грекул, В. И. Проектирование информационных систем: учебник и практикум для вузов / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина. — Москва : Издательство Юрайт, 2022. — 385 с. — (Высшее образование). — ISBN 978-5-9916-8764-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489918
3. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249
4. Казарин О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262

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 «Лань» http://e.lanbook.com/
- 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[3]*:*

1. Курс лекций по дисциплине «Защита сетей и кибербезопасность».
2. Практические задания по дисциплине «Защита сетей и кибербезопасность».

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ

Оценочные материалы и балльно-рейтинговая система[4] оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Защита сетей и кибербезопасность» представлены в Приложении к настоящей Рабочей программе дисциплины.

РАЗРАБОТЧИКИ:

Профессор кафедры прикладной информатики и теории вероятностей		Е.Е. Тимонина
Должность, БУП	Подпись	Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Зав. кафедрой прикладной информатики и теории вероятностей		К.Е. Самуйлов
Наименование БУП	Подпись	Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Зав. кафедрой прикладной информатики и теории вероятностей		К.Е. Самуйлов
Должность, БУП	Подпись	Фамилия И.О.

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

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