

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 28.05.2024 17:18:41

Уникальный программный ключ:

sa953a01204891083f939673078ef1a989dae18a

**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

### КИБЕРПОЛИГОН

(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)

2024 г.

## 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Киберполигон» входит в программу бакалавриата «Кибербезопасность в экономике» по направлению 38.03.05 «Бизнес-информатика» и изучается в 6 семестре 3 курса. Дисциплину реализует Кафедра экономико-математического моделирования. Дисциплина состоит из 3 разделов и 7 тем и направлена на изучение событий и инцидентов информационной безопасности.

Целью освоения дисциплины является получение знания о современных информационных технологиях, получению теоретических знаний и практических навыков эксплуатации отечественных программно-аппаратных комплексов VipNet IDS NS и VipNet TIAS, мониторингу и анализу событий и инцидентов информационной безопасности, практических навыков работы с использованием специального программного обеспечения.

## 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Киберполигон» 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-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;
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	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

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
		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 «Киберполигон» 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 «Киберполигон».

*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	Микроэкономика и менеджмент; Макроэкономика; Международные платежные системы; Экономическая безопасность; Имитационное моделирование угроз экономической кибербезопасности; Бизнес-аналитика и методы принятия решений; Экономика "Умного города" и обеспечение безопасности ее функционирования;	Рынки ИКТ и организация продаж; Электронный бизнес; Искусственный интеллект в бизнесе; Финансовая безопасность; Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика;
ПК-3	Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	Основы программирования; Архитектура компьютеров и операционные системы; Технология программирования; Вычислительные системы, сети и телекоммуникации; Компьютерный практикум; Основы машинного обучения; Основы информатики и кибернетики; Основы информационной безопасности;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Кибербезопасность предприятия;
ПК-4	Способен принимать обоснованные управленческие решения в своей профессиональной деятельности	Микроэкономика и менеджмент; Макроэкономика; Архитектура предприятия; ИТ-инфраструктура предприятия; Моделирование бизнес-	Рынки ИКТ и организация продаж; Электронный бизнес; Искусственный интеллект и кибербезопасность;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
		<p>процессов; Технологии обеспечения кибербезопасности предприятий;</p>	<p>Финансовая безопасность; Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика;</p>
ПК-5	<p>Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем</p>	<p>Имитационное моделирование угроз экономической кибербезопасности; Бизнес-аналитика и методы принятия решений; Экономика "Умного города" и обеспечение безопасности ее функционирования; Экономическая безопасность; Источники угроз кибербезопасности; Технологии обеспечения кибербезопасности предприятий; Противодействие несанкционированным воздействиям в киберпространстве;</p>	<p>Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Искусственный интеллект в бизнесе; Дизайн мышление; Искусственный интеллект и кибербезопасность; Технологии распределенного реестра Blockchain;</p>

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

\*\* - элективные дисциплины /практики

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Киберполигон» 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)
			6
<i>Контактная работа, ак.ч.</i>	54		54
Лекции (ЛК)	18		18
Лабораторные работы (ЛР)	36		36
Практические/семинарские занятия (СЗ)	0		0
<i>Самостоятельная работа обучающихся, ак.ч.</i>	54		54
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	0		0
<b>Общая трудоемкость дисциплины</b>	<b>ак.ч.</b>	<b>108</b>	<b>108</b>
	<b>зач.ед.</b>	<b>3</b>	<b>3</b>

## 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	Комплексный подход к обеспечению информационной безопасности	1.1	Кибербезопасность. Основные понятия и определения. Типы угроз.	ЛК
		1.2	Управление инцидентами информационной безопасности. Технологии обнаружения компьютерных атак	ЛК
Раздел 2	Программные и программно-аппаратные средства обеспечения информационной безопасности	2.1	Сетевой сенсор системы обнаружения атак ПАК ViPNet IDS NS	ЛК, ЛР
		2.2	Системы обнаружения вторжений уровня хоста ViPNet IDS HS	ЛК, ЛР
		2.3	Программно-аппаратный комплекс ViPNet TIAS	ЛК, ЛР
Раздел 3	Мониторинг, анализ и расследование инцидентов с помощью программного комплекса обучения	3.1	Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак	ЛК, ЛР
		3.2	Киберучения на базе программного комплекса	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.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams.
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве 1 шт.), 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 AnyLogic.
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. Дополнительное ПО: офисный пакет MS Office или AnyLogic.
--	---------------------------------	---

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

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### *Основная 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://lib.rudn.ru/MegaPro/UserEntry?Action=Link\\_FindDoc&id=515837&idb=0](https://lib.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=515837&idb=0)

2. Методические материалы для работы с программным комплексом обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire»

3. Руководство администратора. Программно-аппаратный комплекс ViPNet TIAS

4. Выписка из руководства администратора. Программно-аппаратный комплекс для обнаружения вторжений в информационные системы ViPNet IDS NS

5. Методический документ/ Методика оценки угроз безопасности информации (утвержден ФСТЭК России 5.02.2021)

6. Документация на продукты ViPNet представлена в виде pdf-файлов на сайте <https://infotecs.ru/downloads/documentacii/>

### *Дополнительная литература:*

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

2. Дополнительные материалы и учебно-методические комплексы на сайте: <https://infotecs-edu.ru/materials/>

### *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](http://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 «Киберполигон».

\* - 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 «Киберполигон» представлены в Приложении к настоящей Рабочей программе дисциплины.

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

**РАЗРАБОТЧИК:**

Доцент кафедры экономико-  
математического  
моделирования

---

*Должность, БУП*

---

*Подпись*

Решетникова Марина  
Сергеевна

---

*Фамилия И.О.*

**РУКОВОДИТЕЛЬ БУП:**

Заведующий кафедрой  
экономико-математического  
моделирования

---

*Должность БУП*

---

*Подпись*

Балашова Светлана  
Алексеевна

---

*Фамилия И.О.*

**РУКОВОДИТЕЛЬ ОП ВО:**

Заведующий кафедрой теории  
вероятностей и  
кибербезопасности

---

*Должность, БУП*

---

*Подпись*

Самуйлов Константин  
Евгеньевич

---

*Фамилия И.О.*