

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 22.05.2024 14:37:00

Уникальный программный ключ:

sa953a01204891083f939673078ef1a989aae18a

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:

02.03.01 МАТЕМАТИКА И КОМПЬЮТЕРНЫЕ НАУКИ

(код и наименование направления подготовки/специальности)

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

МАТЕМАТИКА И КОМПЬЮТЕРНЫЕ НАУКИ

(наименование (профиль/специализация) ОП ВО)

2024 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Кибербезопасность предприятия» входит в программу бакалавриата «Математика и компьютерные науки» по направлению 02.03.01 «Математика и компьютерные науки» 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-11	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-11.1 Анализирует действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности, а также способы профилактики коррупции и формирования нетерпимого отношения к ней; УК-11.2 Планирует, организует и проводит мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупции в обществе; УК-11.3 Соблюдает правила общественного взаимодействия на основе соблюдения действующего законодательства и нетерпимого отношения к коррупции;
УК-12	Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на	УК-12.1 Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных;

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	основании поступающих информации и данных	
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-5	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-5.1 Знает основные положения и концепции прикладного и системного программирования, архитектуры компьютеров и сетей (в том числе и глобальных), современные языки программирования, технологии создания и эксплуатации программных продуктов и программных комплексов; ОПК-5.2 Умеет использовать основные положения и концепции прикладного и системного программирования, архитектуры компьютеров и сетей (в том числе и глобальных), современные языки программирования, технологии создания и эксплуатации программных продуктов и программных комплексов в профессиональной деятельности; ОПК-5.3 Имеет практические навыки применения современных информационных технологий для решения задач профессиональной деятельности;
ОПК-7	Способен использовать основы экономических знаний в различных сферах жизнедеятельности	ОПК-7.1 Знает базовые основы правовых знаний; ОПК-7.2 Умеет использовать правовые знания в профессиональной деятельности; ОПК-7.3 Имеет практические навыки применения правовых знаний;
ОПК-8	Способен использовать основы правовых знаний в различных сферах жизнедеятельности	ОПК-8.1 Знает базовые принципы по разработке алгоритмов и компьютерных программ, необходимых в профессиональной деятельности в области математики и компьютерных наук для: изучения и моделирования объектов профессиональной деятельности, анализа данных, представления информации и пр. ; ОПК-8.2 Умеет применять необходимые в профессиональной деятельности алгоритмы и методы в области математики и компьютерных наук для: изучения и моделирования объектов профессиональной деятельности, анализа данных, представления информации и пр. ; ОПК-8.3 Владеет необходимыми в профессиональной деятельности технологиями и методами в области математики и компьютерных наук для: изучения и моделирования объектов профессиональной деятельности, анализа данных, представления информации и пр. ;
ПК-1	Способен разрабатывать и отлаживать программный код	ПК-1.1 Знает основы программирования; современные объектно-ориентированные языки программирования; современные структурные языки программирования; языки современных бизнес-приложений; ПК-1.2 Умеет кодировать на языках программирования; тестировать результаты кодирования; ПК-1.3 Владеет навыками разработки кода информационной системы; навыками верификации кода информационной системы;
ПК-2	Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС,	ПК-2.1 Знает инструменты и методы разработки архитектуры, проектирования и дизайна информационных систем; инструменты верификации программного кода; ПК-2.2 Умеет проектировать и верифицировать архитектуру

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	автоматизирующих задачи организационного управления и бизнес-процессы	информационной системы; кодировать на языках программирования; тестировать результаты кодирования; ПК-2.3 Владеет инструментами и методами проектирования и верификации архитектуры информационной системы, разработки и верификации структуры программного кода информационной системы;
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-11	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	Основы военной подготовки. Безопасность жизнедеятельности; Правоведение;	
УК-12	Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения	Обработка данных и визуализация; Основы машинного обучения и нейронные сети; Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);	Технологическая (проектно-технологическая) практика; Преддипломная практика; Научно-исследовательская работа;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
	задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных		
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;	
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; Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);	Преддипломная практика; Научно-исследовательская работа;
ОПК-5	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Архитектура компьютеров и операционные системы; Вычислительные системы, сети и телекоммуникации; Реляционные базы данных; Основы информационной безопасности; Компьютерная геометрия;	Технологическая (проектно-технологическая) практика;
ОПК-7	Способен использовать основы экономических знаний в различных сферах жизнедеятельности	Правоведение; Основы информационной безопасности;	
ОПК-8	Способен использовать основы правовых знаний в различных сферах жизнедеятельности	Вычислительные методы; Математическое моделирование; Имитационное моделирование; Модели мультисервисных сетей с приоритетами; Обработка данных и визуализация; Компьютерная алгебра; Основы машинного обучения и нейронные сети; Компьютерная геометрия; Основы формальных методов описания бизнес-процессов; Введение в управление инфокоммуникациями; Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);	Технологическая (проектно-технологическая) практика;
ПК-1	Способен разрабатывать и	Архитектура компьютеров и	Преддипломная практика;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
	отлаживать программный код	операционные системы; Основы программирования; Технология программирования; Введение в программирование для мобильных платформ; Алгоритмы машинной графики и обработки изображений; <i>Компьютерный практикум по моделированию**</i> ; <i>Компьютерный практикум по информационным технологиям**</i> ; Обработка данных и визуализация; Компьютерная алгебра; Основы машинного обучения и нейронные сети; Компьютерная геометрия; Методы машинного обучения; Машинное обучение в телекоммуникациях;	Научно-исследовательская работа; Технологическая (проектно-технологическая) практика;
ПК-2	Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	Основы программирования; Технология программирования; Технологии искусственного интеллекта; Введение в программирование для мобильных платформ; Методы искусственного интеллекта; Методы машинного обучения; Машинное обучение в телекоммуникациях; <i>Practicum in Artificial Intelligence**</i> ;	Технологическая (проектно-технологическая) практика; Преддипломная практика;
ПК-3	Способен осуществлять администрирование прикладного программного обеспечения, сетевой подсистемы и систем управления базами данных инфокоммуникационной системы организации	Архитектура компьютеров и операционные системы; Вычислительные системы, сети и телекоммуникации; Реляционные базы данных; Основы информационной безопасности; Введение в программирование для мобильных платформ; Методы машинного обучения; Машинное обучение в телекоммуникациях;	Преддипломная практика; Технологическая (проектно-технологическая) 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
<i>Контактная работа, ак.ч.</i>	54		54
Лекции (ЛК)	18		18
Лабораторные работы (ЛР)	0		0
Практические/семинарские занятия (СЗ)	36		36
<i>Самостоятельная работа обучающихся, ак.ч.</i>	54		54
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	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 Х.1205 Обзор кибербезопасности <https://www.itu.int/rec/T-REC-X.1205-200804-I>

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

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

7. Рекомендация МСЭ-Т Х.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 Х.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 Х.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.elsevier.com/locate/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

Должность, БУП

Подпись

Кочеткова Ирина
Андреевна

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой теории
вероятностей и
кибербезопасности

Должность БУП

Подпись

Самуйлов Константин
Евгеньевич

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой теории
вероятностей и
кибербезопасности

Должность, БУП

Подпись

Самуйлов Константин
Евгеньевич

Фамилия И.О.