Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы»

Инженерная академия

(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ТЕХНОЛОГИЧЕСКИЕ УГРОЗЫ И СИСТЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

02.04.02 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):

АНАЛИЗ БОЛЬШИХ ДАННЫХ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

(наименование (профиль/специализация) ОП ВО)

2024 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Технологические угрозы и системы обеспечения кибербезопасности» входит в программу магистратуры «Анализ больших данных и технологии защиты информации» по направлению 02.04.02 «Фундаментальная информатика и информационные технологии» и изучается во 2 семестре 1 курса. Дисциплину реализует Кафедра механики и процессов управления. Дисциплина состоит из 4 разделов и 9 тем и направлена на изучение Диципина направлена на изучение фундаментальных основ моделей угроз информационной безопасности компьютерных систем и оценки их влияния на риски информационной безопасности; разбор основных методов решения типовых задач и знакомство с областью их применения в профессиональной деятельности.

Целью освоения дисциплины является Целью освоения дисциплины является: формирование фундаментальных знаний и навыков применения методов решения задач, необходимых для профессиональной деятельности, повышение общего уровня цифровой грамотности студентов.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Технологические угрозы и системы обеспечения кибербезопасности» 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)
ОПК-5	Способен инсталлировать и сопровождать программное обеспечение информационных систем, осуществлять эффективное управление разработкой программных средств и проектов	ОПК-5.1 Знает порядок и особенности процесса инсталляции программного обеспечения информационных систем;; ОПК-5.2 Умеет обеспечить сопровождение программного обеспечения информационных систем;; ОПК-5.3 Владеет современными информационными технологиями и техническими средствами для осуществления эффективного управления разработкой программных средств и проектов.;
ПК-2	Способен применять методы и технологии защиты информации для решения задач управления проектами в области информационных технологий в условиях неопределенностей и рисков информационных угроз;	ПК-2.1 Знает современные теоретические и экспериментальные методы, применяемые для разработки технологий защиты информации и процессов профессиональной деятельности;; ПК-2.2 Умеет определять эффективность применяемых методов для разработки технологий защиты информации и процессов профессиональной деятельности;; ПК-2.3 Владеет современными теоретическими и экспериментальными методами для разработки технологий защиты информации и процессов профессиональной деятельности.;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Технологические угрозы и системы обеспечения кибербезопасности» 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 «Технологические угрозы и системы обеспечения кибербезопасности».

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

Шифр	**Наименование компетенции**	**Предшествующие дисциплины/модули, практики***	**Последующие дисциплины/модули, практики***
ОПК-5	Способен инсталлировать и сопровождать программное обеспечение информационных систем, осуществлять эффективное управление разработкой программных средств и проектов	Информационные технологии в математическом моделировании; Технологии программирования;	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Научно-исследовательская работа; Преддипломная практика; Интеллектуальные информационные системы;
ПК-2	Способен применять методы и технологии защиты информации для решения задач управления проектами в области информационных технологий в условиях неопределенностей и рисков информационных угроз;	Статистические методы анализа данных; Машинное обучение и анализ больших данных;	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Научно-исследовательская работа; Преддипломная практика; Криптология и практика шифрования; Защищенное программное обеспечение; *Искусственные нейронные сети (Обучение с подкреплением)***; *Artificial Neural Networks (Reinforcement Learning)***;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Технологические угрозы и системы обеспечения кибербезопасности» составляет «8» зачетных единиц.

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)**
			2
Контактная работа, ак.ч.	*72*		*72*
Лекции (**ЛК**)	36		36
Лабораторные работы (**ЛР**)	36		36
Практические/семинарские занятия (**СЗ**)	0		0
Самостоятельная работа обучающихся, ак.ч.	*189*		*189*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
Общая трудоемкость дисциплины	**ак.ч.**	***288***	*288*
	зач.ед.	***8***	*8*

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	Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей КС	1.1	Стандарты и нормативные документы	ЛК, ЛР
		1.2	Уязвимости информационных систем. Классификация уязвимостей информационных систем.	ЛК, ЛР
Раздел 2	Механизмы нарушения ИБ КС	2.1	Несанкционированный доступ к информации	ЛК, ЛР
		2.2	Утечки информации по техническим каналам	ЛК, ЛР
Раздел 3	Оценка угроз нарушения ИБ КС	3.1	Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности	ЛК, ЛР
		3.2	Оценка актуальности угроз безопасности информации	ЛК, ЛР
		3.3	Оценка уровня опасности уязвимостей информационных компонентов инфокоммуникационных систем	ЛК, ЛР
Раздел 4	Способы защиты КС от угроз ИБ	4.1	Система менеджмента информационной безопасности. Оценка рисков информационной безопасности.	ЛК, ЛР
		4.2	Аппаратно-программные средства защиты информации в КС.	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 [Параметр] шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	
Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и	

	консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Галатенко, В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко. — 3-е изд. — Электрон. текстовые данные — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. — 266 с.
2. Шаньгин В.Ф. Информационная безопасность и защита информации / Шаньгин В.Ф. — 2-е изд. — Электрон. текстовые данные. — Саратов: Профобразование, 2019. — 702 с.

Дополнительная литература:

1. Нестеров С.А. Основы информационной безопасности: учебное пособие/ Нестеров С.А. — Электрон. текстовые данные. — СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с.

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 «Технологические угрозы и системы обеспечения кибербезопасности».

* - 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 «Технологические угрозы и системы обеспечения кибербезопасности» представлены в Приложении к настоящей Рабочей программе дисциплины.

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

РАЗРАБОТЧИК:

Доцент		Варфоломеев Александр Алексеевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой		Разумный Юрий Николаевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Доцент		Варфоломеев Александр Алексеевич
Должность, БУП	*Подпись*	*Фамилия И.О.*