

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ястребов Олег Александрович
Должность: Ректор
Дата подписания: 10.06.2025 09:07:52
Уникальный программный ключ:
sa953a0120d891083f939673078ef1a989dae18a

**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

TECHNOLOGY THREATS AND CYBERSECURITY SYSTEMS

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

27.04.04 УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ СИСТЕМАХ

(код и наименование направления подготовки/специальности)

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

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ, МАШИННОЕ ОБУЧЕНИЕ И КОСМИЧЕСКИЕ НАУКИ

(наименование (профиль/специализация) ОП ВО)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Technology Threats and Cybersecurity Systems» входит в программу магистратуры «Искусственный интеллект, машинное обучение и космические науки» по направлению 27.04.04 «Управление в технических системах» и изучается в 3 семестре 2 курса. Дисциплину реализует Кафедра механики и процессов управления. Дисциплина состоит из 4 разделов и 9 тем и 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 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 «Technology Threats and Cybersecurity Systems» 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-10	Способен руководить разработкой методических и нормативных документов, технической документации в области автоматизации технологических процессов и производств, в том числе по жизненному циклу продукции и ее качеству	ОПК-10.1 Знаком с основными подходами к разработке методических и нормативных документов, технической документации в области автоматизации технологических процессов и производств;; ОПК-10.2 Владеет подходами для руководства разработкой технической документации и нормативных документов в области автоматизации технологических процессов и производств, в том числе по жизненному циклу продукции и ее качеству;
ОПК-6	Способен осуществлять сбор и проводить анализ научно-технической информации, обобщать отечественный и зарубежный опыт в области средств автоматизации и управления	ОПК-6.1 Знает основные методы сбора и проведения анализа научно-технической информации;; ОПК-6.2 Умеет анализировать и обобщать отечественный и зарубежный опыт в области средств автоматизации и управления;; ОПК-6.3 Владеет методами сбора и проведения анализа научно-технической информации, а также может обобщать отечественный и зарубежный опыт в профессиональной отрасли;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Technology Threats and Cybersecurity Systems» 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 «Technology Threats and Cybersecurity Systems».

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-6	Способен осуществлять сбор и проводить анализ научно-технической информации, обобщать отечественный и зарубежный опыт в области средств автоматизации и управления	Research work / Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Relational Database Management System; Python for Data Science; Inferential Statistics;	Undergraduate practice / Преддипломная практика;
ОПК-10	Способен руководить разработкой методических и нормативных документов, технической документации в области автоматизации технологических процессов и производств, в том числе по жизненному циклу продукции и ее качеству	Research work / Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);	Undergraduate practice / Преддипломная практика;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Technology Threats and Cybersecurity Systems» 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)
			3
Контактная работа, ак.ч.	34		34
Лекции (ЛК)	17		17
Лабораторные работы (ЛР)	17		17
Практические/семинарские занятия (СЗ)	0		0
Самостоятельная работа обучающихся, ак.ч.	38		38
Контроль (экзамен/зачет с оценкой), ак.ч.	36		36
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	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 15 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. Maglaras L., Kantzavelou I. (ed.). Cybersecurity issues in emerging technologies. – CRC press, 2021.

2. Sarfraz M. (ed.). Cybersecurity Threats with New Perspectives. – BoD–Books on Demand, 2021.

Дополнительная литература:

1. Toch E. et al. The privacy implications of cyber security systems: A technological survey //ACM Computing Surveys (CSUR). – 2018. – Т. 51. – №. 2. – С. 1-27.

2. Jang-Jaccard J., Nepal S. A survey of emerging threats in cybersecurity //Journal of computer and system sciences. – 2014. – Т. 80. – №. 5. – С. 973-993.

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/>

- Научометрическая база данных Lens.org <https://www.lens.org>

Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля:*

1. Курс лекций по дисциплине «Technology Threats and Cybersecurity Systems».

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

РАЗРАБОТЧИК:

Доцент

Должность, БУП

Подпись

Варфоломеев Александр

Алексеевич

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой

Должность, БУП

Подпись

Разумный Юрий
Николаевич [М](вн.

совм.) заведующий

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой

Должность, БУП

Подпись

Разумный Юрий

Николаевич

Фамилия И.О.