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:

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):

АНАЛИЗ БОЛЬШИХ ДАННЫХ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

(наименование (профиль/специализация) ОП ВО)

2026 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 27.04.04 «Управление в технических системах» 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 Дициплина 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-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-9	Способен разрабатывать методики и выполнять эксперименты на действующих объектах с обработкой результатов на основе информационных технологий и технических средств	ОПК-9.1 Владеет современными информационными технологиями и техническими средствами для проведения экспериментов на действующих объектах;; ОПК-9.2 Имеет навыки разработки методик и выполнения экспериментов на действующих объектах;; ОПК-9.3 Имеет навыки разработки методик и выполнения экспериментов на действующих объектах с обработкой результатов посредством информационных технологий.;
ПК-3	Способен определять угрозы безопасности информации и возможные пути ее защиты на основе анализа структуры и содержания информационных процессов и особенностей функционирования информационной системы	ПК-3.1 Умеет проводить анализ структуры и содержания информационных процессов и особенностей функционирования информационных систем;; ПК-3.2 Умеет формулировать рекомендации по совершенствованию информационных систем и технологий защиты их безопасности от угроз;; ПК-3.3 Владеет методами решения профессиональных задач в области защиты информации и информационных систем.;

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-9	Способен разрабатывать методики и выполнять эксперименты на действующих объектах с обработкой результатов на основе информационных технологий и технических средств	Информационные технологии в математическом моделировании; Машинное обучение и анализ больших данных; Статистические методы анализа данных;	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); 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		Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Преддипломная практика;
ПК-3	Способен определять угрозы безопасности информации и возможные пути ее защиты на основе анализа структуры и содержания информационных процессов и особенностей функционирования информационной системы		Научно-исследовательская работа; Преддипломная практика; Динамика и управление космическими системами; *Искусственные нейронные сети (Обучение с подкреплением)***; *Artificial Neural Networks (Reinforcement Learning)***; Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);

* - 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	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 1	Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей КС	1.1	Стандарты и нормативные документы	Международные и национальные стандарты информационной безопасности. Серия ISO/IEC 27000. Нормативные документы ФСТЭК России и ФСБ России. Доктрина информационной безопасности Российской Федерации. Классификация угроз безопасности информации.	ЛК
		1.2	Уязвимости информационных систем. Классификация уязвимостей информационных систем.	Понятие уязвимости информационной системы. Классификация уязвимостей по природе возникновения: аппаратные, программные, организационные. Классификация по этапу жизненного цикла. Базы данных уязвимостей CVE и NVD. Система оценки критичности уязвимостей CVSS.	ЛК, ЛР
Раздел 2	Механизмы нарушения ИБ КС	2.1	Несанкционированный доступ к информации	Понятие несанкционированного доступа. Классификация нарушителей. Типовые способы несанкционированного доступа. Методы предотвращения: идентификация, аутентификация, разграничение доступа, регистрация событий.	ЛК, ЛР
		2.2	Утечки информации по техническим каналам	Понятие технического канала утечки информации. Акустические, виброакустические, оптические каналы. Побочные электромагнитные излучения и наводки. Каналы утечки через цепи электропитания и заземления. Методы защиты: экранирование, фильтрация, зашумление.	ЛК, ЛР
Раздел 3	Оценка угроз нарушения ИБ КС	3.1	Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности	Понятие угрозы безопасности информации. Источники угроз. Методики оценки возможности реализации угроз. Определение актуальных угроз для информационной системы.	ЛК, ЛР
		3.2	Оценка актуальности угроз безопасности информации	Критерии отнесения угроз к актуальным. Анализ вероятности реализации угрозы. Ранжирование угроз. Построение модели угроз для информационной системы.	ЛК, ЛР
		3.3	Оценка уровня опасности уязвимостей информационных компонентов инфокоммуникационных систем	Понятие уровня опасности уязвимости. Методика CVSS. Базовые, временные и средовые метрики. Интерпретация оценки: низкий, средний, высокий, критический уровень опасности.	ЛК, ЛР
Раздел 4	Способы защиты КС от угроз ИБ	4.1	Система менеджмента информационной безопасности. Оценка рисков информационной безопасности.	Система менеджмента информационной безопасности СМИБ. Стандарт ISO/IEC 27001. Понятие риска информационной безопасности. Методологии оценки рисков: количественная и	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				качественная. Матрица рисков. Обработка рисков.	
		4.2	Аппаратно-программные средства защиты информации в КС.	Классификация средств защиты. Средства идентификации и аутентификации. Средства разграничения доступа. Межсетевые экраны. Средства обнаружения и предотвращения вторжений. Антивирусные средства. Криптографические средства. Средства защиты от утечек информации DLP. Системы управления событиями безопасности SIEM.	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 ____ 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 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/
   - Наукометрическая база данных Lens.org https://www.lens.org

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**!

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:

Профессор		Разумный Юрий Николаевич
Должность, БУП	*Подпись*	*Фамилия И.О.*