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

ОСНОВЫ ТЕХНОЛОГИЧЕСКИХ УГРОЗ И КИБЕРБЕЗОПАСНОСТИ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

27.03.04 УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ СИСТЕМАХ
(код и наименование направления подготовки/специальности)

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

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ ПРОЦЕССАМИ, МАШИННОЕ ОБУЧЕНИЕ И КИБЕРБЕЗОПАСНОСТЬ
(наименование (профиль/специализация) ОП ВО)

2023 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Основы технологических угроз и кибербезопасности» входит в программу бакалавриата «Управление информационными процессами, машинное обучение и кибербезопасность» по направлению 27.03.04 «Управление в технических системах» и изучается в 5 семестре 3 курса. Дисциплину реализует Департамент механики и процессов управления. Дисциплина состоит из 8 разделов и 26 тем и направлена на изучение основных методик и подходов к обеспечению кибербезопасности в рамках современных автоматизированных систем; знакомство с принципыпами построения защищенных информационных систем и поддержания подсистемы защиты информации в актуальном состоянии; особенностей реализации общих методик защиты информации на различных платформах.

Целью освоения дисциплины является сформировать компетенции обучающегося в области кибербезопасности, заложить терминологический фундамент и ознакомить с общими методами и подходами обеспечения информационной безопасности

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Основы технологических угроз и 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-11	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-11.1 Знает цифровые методы и технологии применяемые в профессиональной деятельности; ОПК-11.2 Умеет применять цифровые методы и технологии в профессиональной деятельности для изучения и моделирования объектов профессиональной деятельности, анализа данных, представления информации; ОПК-11.3 Уверенно владеет цифровыми методами и технологиями в профессиональной деятельности (в области управления в технических системах) для: изучения и моделирования объектов профессиональной деятельности, анализха данных, представления информации;
ПК-7	Способен разрабатывать и анализировать проектные решения по обеспечению кибербезопасности автоматизированных систем	ПК-7.1 Знает основные подходы к разработке проектных решений по обеспечению кибербезопасности информационных систем; ПК-7.2 Умеет анализировать проектные решения на предмет обеспечения кибербезопасности; ПК-7.3 Владеет техниками реализации проектных решений, обеспечивающих кибербезопасность автоматизированных систем;
ПК-9	Способен обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований кибербезопасности	ПК-9.1 Знает основные информационно-технологические ресурсы автоматизированных систем для обеспечения кибербезопасноси; ПК-9.2 Умеет выделять наиболее значимые информационно-технологические ресурсы автоматизированных систем; ПК-9.3 Владеет технологиями для обеспечния эффективного применения информационно-технологических ресурсов астоматизированных систем с учетом обеспечения кибербезопасности;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Основы технологических угроз и 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 «Основы технологических угроз и 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-11	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Информатика и программирование; Механика космического полета; Анализ геоинформационных данных;	Методы оптимального управления; Анализ данных и машинное обучение; Преддипломная практика; Технологическая практика;
ПК-7	Способен разрабатывать и анализировать проектные решения по обеспечению кибербезопасности автоматизированных систем		Проектная практика; Основы информационной безопасности и киберустойчивости; Основы разработки защищенного программного обеспечения и компьютерных сетей;
ПК-9	Способен обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований кибербезопасности		

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Основы технологических угроз и кибербезопасности» составляет «7» 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)**
			5
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.	*144*		*144*
Контроль (экзамен/зачет с оценкой), ак.ч.	*36*		*36*
Общая трудоемкость дисциплины	**ак.ч.**	***252***	*252*
	зач.ед.	***7***	*7*

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	Введение в информационную безопасность	1.1	Основные определения и понятия кибербезопасности	ЛК
		1.2	Классификация технологических угроз	ЛК
Раздел 2	Общеметодологические принципы теории информационной безопасности	2.1	Этапы развития информационной безопасности: - системы безопасности ресурса; - развитой защиты (комплексирования целей защиты, расширение арсенала используемых средств защиты, объединение в функциональные самостоятельные системы защиты); -Этап комплексной защиты.	ЛК, ЛР
		2.2	Требования к системе защиты информации. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Комплексность: целевая, инструментальная, структурная, функциональная, временная	ЛК, ЛР
Раздел 3	Классификация угроз информационной безопасности	3.1	Основные типы и причины угроз информационной безопасности	ЛК
		3.2	Их классификация	ЛК
Раздел 4	Виды противников и каналы утечки информации	4.1	Виды возможных противников	ЛК, ЛР
		4.2	Возможные каналы утечки информации	ЛК, ЛР
Раздел 5	Политика безопасности информационных систем	5.1	Этапы построения системы защиты информации	ЛК, ЛР
		5.2	Политика безопасности	ЛК
		5.3	Оценка эффективности инвестиций в информационную безопасность	ЛК, ЛР
		5.4	Обеспечение информационной безопасности автоматизированных банковских систем	ЛК, ЛР
		5.5	Информационная безопасность электронной коммерции	ЛК, ЛР
		5.6	Обеспечение компьютерной безопасности учетной информации	ЛК, ЛР
Раздел 6	Организационно-правовые методы защиты информации	6.1	Организационные основы защиты информации	ЛК, ЛР
		6.2	Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений	ЛК
		6.3	Организация допуска и доступа персонала к конфиденциальной информации	ЛК, ЛР
		6.4	Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации	ЛК, ЛР
		6.5	Организация внутриобъектового и пропускного режимов на предприятии	ЛК, ЛР
		6.6	Правовая защита конфиденциальной информации	ЛК, ЛР
Раздел 7	Программно- аппаратные методы защиты информации	7.1	Идентификация и аутентификация. Управление доступом	ЛК, ЛР
		7.2	Протоколирование и аудит	ЛК, ЛР
		7.3	Криптография	ЛК, ЛР
		7.4	Экранирование	ЛК, ЛР
Раздел 8	Стандарты обеспечения информационной безопасности	8.1	Международные стандарты кибербезопасности	ЛК
		8.2	Российские стандарты кибербезопасности	ЛК

* - заполняется только по **ОЧНОЙ** форме обучения: *ЛК – лекции; ЛР – лабораторные работы; СЗ – 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.
2.

Дополнительная литература:

1.
2.

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 «Основы технологических угроз и 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 «Основы технологических угроз и 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:

Директор ДМПУ		Разумный Юрий Николаевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

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