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):

DATA ENGINEERING, ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ И КИБЕРБЕЗОПАСНОСТЬ

(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Основы технологических угроз и кибербезопасности» входит в программу бакалавриата «Data Engineering, интеллектуальные системы и кибербезопасность» по направлению 27.03.04 «Управление в технических системах» и изучается в 5 семестре 3 курса. Дисциплину реализует Кафедра 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, анализа 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 кибербезопасности; ПК-9.2 Умеет выделять наиболее значимые информационно-технологические ресурсы автоматизированных систем; ПК-9.3 Владеет технологиями для обеспечения эффективного применения информационно-технологических ресурсов автоматизированных 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	Механика космического полета;	Методы оптимального управления; Применение технологий искусственного интеллекта в механике и процессах управления; Технологическая практика (учебная); Научно-исследовательская работа; Преддипломная 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 «4» 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)**
			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.	*45*		*45*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
Общая трудоемкость дисциплины ак.ч.	**ак.ч.**	**144**	**144**
	зач.ед.	**4**	**4**

Общая трудоемкость дисциплины «Основы технологических угроз и кибербезопасности» составляет «4» зачетные единицы

Таблица 4.2. Виды учебной работы по периодам освоения образовательной программы высшего образования для заочной формы обучения.

Вид учебной работы	**ВСЕГО, ак.ч.**		**Семестр(-ы)**	**Семестр(-ы)**	**Семестр(-ы)**	**Семестр(-ы)**
			5	**6**	**7**	**8**
Контактная работа, ак.ч	*28*		*4*	*8*	*8*	*8*
Лекции (**ЛК**)	14		2	4	4	4
Лабораторные работы (**ЛР**)	14		2	4	4	4
Практические/семинарские занятия (**СЗ**)	0		0	0	0	0
Самостоятельная работа обучающихся, ак.ч.	*107*		*32*	*28*	*28*	*19*
Контроль (экзамен/зачет с оценкой), ак.ч.	*9*		*0*	*0*	*0*	*9*
Общая трудоемкость дисциплины ак.ч.	**ак.ч.**	**144**	**36**	**36**	**36**	**36**
	зач.ед.	**4**	**1**	**1**	**1**	**1**

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	Введение в информационную безопасность	1.1	Основные определения и понятия кибербезопасности	Кибербезопасность как совокупность методов и практик защиты цифровых систем, сетей и данных от кибератак. Основные понятия: конфиденциальность, целостность, доступность информации. Угроза, уязвимость, риск, атака. Отличие кибербезопасности от информационной безопасности.	ЛК
		1.2	Классификация технологических угроз	Технологические угрозы как риски, связанные с использованием информационных и коммуникационных технологий. Классификация по источнику: внешние и внутренние. По характеру воздействия: случайные и умышленные. По объекту воздействия: аппаратное, программное обеспечение, данные, сетевые коммуникации.	ЛК
Раздел 2	Общеметодологические принципы теории информационной безопасности	2.1	Этапы развития информационной безопасности	Системы безопасности ресурса с акцентом на защиту отдельных объектов. Развитая защита с комплексированием целей защиты, расширением арсенала используемых средств защиты, объединением в единые системы управления безопасностью. Проактивная защита с прогнозированием и предотвращением угроз.	ЛК, ЛР
		2.2	Требования к системе защиты информации.	Показатели информации: важность как ценность информации для владельца, полнота как достаточность для принятия решений, адекватность как соответствие реальному положению дел, релевантность как соответствие запросу, толерантность как устойчивость к ошибкам. Комплексность защиты: целевая согласованность целей, инструментальная разнообразие средств, структурная охват всех элементов, функциональная непрерывность защиты.	ЛК, ЛР
Раздел 3	Классификация угроз информационной безопасности	3.1	Основные типы и причины угроз информационной безопасности	Показатели информации: важность как ценность информации для владельца, полнота как достаточность для принятия решений, адекватность как соответствие реальному положению дел, релевантность как соответствие запросу, толерантность как устойчивость к ошибкам. Комплексность защиты: целевая согласованность целей, инструментальная разнообразие средств, структурная охват всех элементов, функциональная непрерывность защиты.	ЛК
		3.2	Их классификация	Классификация угроз по масштабу: локальные, региональные, глобальные. По способу воздействия: прямые и косвенные. По используемым уязвимостям: аппаратные, программные, сетевые, человеческие. По последствиям: нарушение конфиденциальности, целостности, доступности.	ЛК
Раздел 4	Виды противников и каналы утечки информации	4.1	Виды возможных противников	Хакеры, киберпреступники, конкуренты, иностранные спецслужбы, недобросовестные сотрудники, террористические организации. Мотивы и возможности различных категорий противников.	ЛК, ЛР
		4.2	Возможные каналы утечки информации	Каналы утечки информации: технические акустические, визуально-оптические, электромагнитные. Организационные каналы: через персонал, документы, переписку. Сетевые каналы: перехват трафика, несанкционированный доступ к ресурсам.	ЛК, ЛР
Раздел 5	Политика безопасности информационных систем	5.1	Этапы построения системы защиты информации	Анализ рисков, разработка концепции защиты, выбор средств защиты, внедрение, эксплуатация и сопровождение, аудит и совершенствование.	ЛК, ЛР
		5.2	Политика безопасности	Политика безопасности как совокупность правил, процедур и практик, регулирующих управление, защиту и распределение информационных активов. Документы политики безопасности: стратегия, регламенты, инструкции.	ЛК

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
		5.3	Оценка эффективности инвестиций в информационную безопасность	Методы расчёта возврата инвестиций в безопасность. Сравнение затрат на внедрение средств защиты с потенциальным ущербом от реализации угроз.	ЛК, ЛР
		5.4	Обеспечение информационной безопасности автоматизированных банковских систем	Особенности обеспечения безопасности автоматизированных банковских систем. Защита межбанковских переводов, платёжных шлюзов, процессинговых центров. Требования регуляторов Центрального банка.	ЛК, ЛР
		5.5	Информационная безопасность электронной коммерции	Защита платежных данных клиентов. Обеспечение безопасности интернет-магазинов, платёжных агрегаторов, маркетплейсов. Стандарт PCI DSS.	ЛК, ЛР
		5.6	Обеспечение компьютерной безопасности учетной информации	Хранение учётных данных. Политика управления паролями. Многофакторная аутентификация.	ЛК, ЛР
Раздел 6	Организационно-правовые методы защиты информации	6.1	Организационные основы защиты информации	Создание службы безопасности, распределение ответственности, организация режима секретности, обучение персонала, контроль соблюдения правил.	ЛК, ЛР
		6.2	Отнесение сведений к конфиденциальной информации.	Засекречивание и рассекречивание сведений. Порядок допуска к государственной тайне.	ЛК
		6.3	Организация допуска и доступа персонала к конфиденциальной информации	Оформление допуска. Разграничение прав доступа в соответствии с должностными обязанностями.	ЛК, ЛР
		6.4	Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации	Инструктажи, обучение, проверка лояльности. Ответственность за разглашение.	ЛК, ЛР
		6.5	Организация внутриобъектового и пропускного режимов на предприятии	Контроль входа и выхода сотрудников и посетителей. Пропускная система. Зонирование территории по степени доступа.	ЛК, ЛР
		6.6	Правовая защита конфиденциальной информации	Гражданско-правовая, административная и уголовная ответственность за нарушения. Защита коммерческой и служебной тайны.	ЛК, ЛР
Раздел 7	Программно- аппаратные методы защиты информации	7.1	Идентификация и аутентификация. Управление доступом	Аутентификация как проверка подлинности субъекта. Управление доступом как разрешение или запрет доступа к ресурсам на основе политики безопасности.	ЛК, ЛР
		7.2	Протоколирование и аудит	Аудит как анализ журналов для выявления нарушений и инцидентов. Сбор, хранение и защита журналов событий.	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
		7.3	Криптография	Криптография как наука о методах шифрования информации. Симметричное и асимметричное шифрование. Электронная подпись для подтверждения подлинности и целостности данных. Хеширование.	ЛК, ЛР
		7.4	Экранирование	Экранирование как ограничение доступа между сетями или сегментами сети. Межсетевые экраны. Фильтрация трафика по правилам. Защита периметра сети.	ЛК, ЛР
Раздел 8	Стандарты обеспечения информационной безопасности	8.1	Международные стандарты кибербезопасности	Международные стандарты кибербезопасности: ISO/IEC 27000 series по менеджменту информационной безопасности. NIST Cybersecurity Framework. PCI DSS для платёжных систем. COBIT для управления ИТ.	ЛК
		8.2	Российские стандарты кибербезопасности	Российские стандарты кибербезопасности: ГОСТ Р ИСО/МЭК 15408 Общие критерии. ГОСТ Р ИСО/МЭК 27001.	ЛК

* - 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 14 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. Белов А. С. Модернизация системы информационной безопасности = Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. - 2022. - № 4. - С. 76-80.

2. Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления / А. Ю. Пучков, А. М. Соколов, С. С. Широков, Н. Н. Прокимнов // Прикладная информатика. - 2023. - Т. 18, № 2. - С. 85-102.

3. Галатенко, В. А. Основы информационной безопасности [Электронный ресурс] / В. А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — 978-5-94774-821-5. — Режим доступа: http://www.iprbookshop.ru/52209.html

4. Ермаков, Д. Г. Применение антивирусных программ для обеспечения информационной безопасности / Д. Г. Ермаков, А. В. Присяжный. — Екатеринбург : Уральский федеральный университет, ЭБС АСВ, 2013. — 64 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/66577.html

5. Костин, В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 31 с. — ISBN 978-5-906953-53-7. — Текст :электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/98200.html

Дополнительная литература:

1. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Москва, Вологда : Инфра-Инженерия, 2020. — 692 с. —ISBN 978-5-9729-0486-0. — Текст : электронный // Электронно-библиотечная система IPRBOOKS : [сайт]. — URL: http://www.iprbookshop.ru/983

2. Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя; перевод с английского Д. А. Беликова. -Москва: ДМК Пресс, 2020. - 326 с. -ISBN 978-5-97060-709-1.- Текст:электронный//Лань: электроннобиблиотечная система. -URL:https://e.lanbook.com/book/131717

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**!

РАЗРАБОТЧИКИ

Доцент	Варфоломеев А.А.
Должность	Фамилия И.О

РУКОВОДИТЕЛЬ БУП

Заведующий кафедрой	Разумный Ю.Н.
Должность	Фамилия И.О

РУКОВОДИТЕЛЬ ОП ВО

Профессор	Разумный Ю.Н.
Должность	Фамилия И.О