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 ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРУСТОЙЧИВОСТИ
(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 информационной безопасности и киберустойчивости» входит в программу бакалавриата «Управление информационными процессами, машинное обучение и кибербезопасность» по направлению 27.03.04 «Управление в технических системах» и изучается в 6 семестре 3 курса. Дисциплину реализует Департамент механики и процессов управления. Дисциплина состоит из 13 разделов и 32 тем и направлена на изучение основных видов возможных технологических угроз и способов обеспечения информационной безопасности

Целью освоения дисциплины является получение знаний, умений, навыков и опыта деятельности в области обеспечения информационной безопасности и защиты информации

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Основы информационной безопасности и киберустойчивости» 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-2	Способен формулировать задачи профессиональной деятельности на основе знаний, профильных разделов математических и естественнонаучных дисциплин (модулей)	ОПК-2.1 Определяет задачи профессиональной деятельности с позиции профильных разделов математических и естетственнонаучных дисциплин; ОПК-2.2 Умеет использовать знания профильных разделов математических и естетсвеннонаучных дисциплин для формулировки задач профессиональной деятельности; ОПК-2.3 Применяет знания профильных разделов математических и естественнонаучных дисциплин для разработки алгоритма решения задач профессиональной деятельности;
ОПК-5	Способен решать задачи развития науки, техники и технологии в области управления в технических системах с учетом нормативно-правового регулирования в сфере интеллектуальной собственности	ОПК-5.1 Определяет цели для решения задач развития науки, техники и технологий в области управления в технических системах; ОПК-5.2 Знает и использует методы для решения задач развития науки, техники и технологий в области упрвления в технических системах с учетом нормативно-правового регулирования в сфере интеллектуальной собственности; ОПК-5.3 Обеспечивает решение задач развития науки, техники и технологии в области управления в технических системах с учетом нормативно-правового регулирования в сфере интеллектуальной собственности;
ПК-10	Способен применять информационные технологии, соблюдать основные требования информационной безопасности	ПК-10.1 Знает основные подходы и методы сбора и анализа исходных данных для расчета и проектирования систем и средств автоматизации и управления; ПК-10.2 Умеет применять информационные технологии в профессиональной деятельности, соблюдать основные требования информационной безопасности; ПК-10.3 Владеет современными информационными технологиями для расчета и проектирования систем и средств автоматизации и управления;
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;

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
		ПК-7.3 Владеет техниками реализации проектных решений, обеспечивающих кибербезопасность автоматизированных систем;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Основы информационной безопасности и киберустойчивости» 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 информационной безопасности и киберустойчивости».

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-2	Способен формулировать задачи профессиональной деятельности на основе знаний, профильных разделов математических и естественнонаучных дисциплин (модулей)	Физика; Теория автоматического управления; Электротехника и электроника; Математический анализ; Алгебра и геометрия; Комплексный анализ; Теория вероятностей и математическая статистика; Информатика и программирование;	Преддипломная практика; Уравнения математической физики;
ОПК-5	Способен решать задачи развития науки, техники и технологии в области управления в технических системах с учетом нормативно-правового регулирования в сфере интеллектуальной собственности	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Теоретическая механика; Механика космического полета;	Преддипломная практика; Правовые основы искусственного интеллекта; Методы оптимального управления;
ПК-10	Способен применять информационные технологии, соблюдать основные требования информационной безопасности		Основы разработки защищенного программного обеспечения и компьютерных сетей; Преддипломная практика; Технологическая практика;
ПК-7	Способен разрабатывать и анализировать проектные решения по обеспечению кибербезопасности автоматизированных систем	Основы технологических угроз и кибербезопасности;	Основы разработки защищенного программного обеспечения и компьютерных сетей;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Основы информационной безопасности и киберустойчивости» 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)**
			6
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.**	***144***	*144*
	зач.ед.	***4***	*4*

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	Сущность, задачи и проблемы информационной безопасности	1.1	Введение. Роль информации в жизнедеятельности современного общества. Развитие информационной индустрии. Объективная необходимость информационной безопасности и защиты информации.	ЛК, ЛР
		1.2	Определение информации. Документированная информация. Электронное сообщение. Активы. Ресурсы. ¶Различные определения информационной безопасности, защиты информации, кибербезопасности, киберустойчивости¶	ЛК, ЛР
		1.3	Современная постановка задачи защиты информации. ¶Назначение и структура дисциплины. Рекомендуемая основная и дополнительная литература. Интернет-источники. Специалисты по обеспечению информационной безопасности. Лицензирование деятельности по обеспечению информационной безопасности.¶	ЛК, ЛР
Раздел 2	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ	2.1	Органы, обеспечивающие национальную безопасность РФ, цели, задачи.	ЛК, ЛР
		2.2	Национальные интересы РФ в информационной сфере. Приоритетные направления в области защиты информации в РФ.	ЛК, ЛР
		2.3	Тенденции развития информационной политики государств и ведомств. Государственная тайна.	ЛК, ЛР
Раздел 3	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности	3.1	Общие положения. Концептуальные документы в области информационной безопасности. Важнейшие федеральные нормативные правовые акты. Законы, касающиеся охраны интеллектуальной собственности. Положения Гражданского кодекса РФ по защите информации.	ЛК, ЛР
		3.2	Международное сотрудничество. Кодекс об административных правонарушениях. Уголовный кодекс и защита информации. Основные подзаконные акты в области информационной безопасности. Указы Президента РФ, постановления Правительства РФ, ведомственная нормативная база.	ЛК, ЛР
Раздел 4	Угрозы информационной безопасности. Управление рисками.	4.1	Понятие угрозы. Виды угроз. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. ¶Модель угроз и модель нарушителя информационной безопасности. ¶	ЛК, ЛР
		4.2	Общая характеристика анализа, оценки и управления рисками. Шкалы. Оценка на основе выявления слабого звена. Оценка рисков на основе рассмотрения этапов вторжения. Программные средства, используемые для анализа рисков.	ЛК, ЛР
Раздел 5	Информационные и автоматизированные системы	5.1	Определения информационной (ИС) и автоматизированной системы (АС) обработки информации. ГОСТы на АС. Типовые виды структуры АС. Виды воздействия на информацию в ИС и АС. Угрозы безопасности	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			АС и их классификация.	
		5.2	Меры противодействия угрозам безопасности АС. Уязвимости АС. Принципы построения системы защиты АС. Автоматизированные системы управления технологическими процессами (АСУ ТП).	ЛК, ЛР
Раздел 6	Технические каналы утечки информации	6.1	Технические каналы утечки информации (ТКУИ) и способы их перекрытия. Пассивная и активная защита от утечки информации по техническим каналам. Определение, классификация и общая характеристика ТКУИ.	ЛК, ЛР
		6.2	Визуальные и акустические каналы. Защита информации в телефонных каналах. Защита от побочных электромагнитных излучений и наводок (ПЭМИН). Технические закладки.	ЛК, ЛР
		6.3	Способы обнаружения ТКУИ. Способы и методы перекрытия ТКУИ. Требования к выбору и оборудованию помещений для АС обработки данных по условиям защиты от ТКУИ. Понятие контролируемой территории и методы определения ее размеров. Особенности защиты персональной вычислительной техники от утечки информации по техническим каналам.	ЛК, ЛР
Раздел 7	Технические средства обеспечения безопасности объекта.	7.1	Определение и основные цели защиты современных объектов. Технические средства обеспечения защиты объекта: определение, системная классификация, общий анализ. Технические средства и системы охраны территории, зданий и помещений.	ЛК, ЛР
		7.2	Технические средства наблюдения и контроля за перемещением людей и предметов. Технические средства и системы опознавания людей. Технические средства и системы управления доступом на территорию, в здания и помещения, к средствам обработки и хранения информации. Методы выбора технических средств, общие сведения о рынке технических средств обеспечения безопасности.	ЛК, ЛР
Раздел 8	Методы контроля доступа к информации	8.1	Методы идентификации и аутентификации пользователей. Метод паролей. Биометрическая аутентификация. Способы разграничения доступа, методы и средства их реализации.	ЛК, ЛР
		8.2	Краткая характеристика современных средств разграничения доступа. Математические модели управления доступом к информации. Субъектно-объектная модель доступа.	ЛК, ЛР
		8.3	Политика безопасности и модель доступа. Электронные ключи. Идентификационные карточки, брелоки. Типы карточек. Единая биометрическая система России.	ЛК, ЛР
Раздел 9	Вредоносные программы	9.1	Вредоносные закладки (ВЗ): определение, разновидности. Разрушающие действия закладок. Системы разграничения доступа и защиты от ВЗ. Предупреждение и минимизация последствий воздействия ВЗ.	ЛК, ЛР
		9.2	Краткая характеристика мер защиты: правовые, административные и организационные, аппаратно-программные. Компьютерные вирусы. Классификация	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
		9.3	Основные каналы распространения вирусов и других вредоносных программ. Средства борьбы с вирусами: краткая характеристика популярных антивирусных программ.¶Средства защиты от копирования. Примеры средств и технологий¶	ЛК, ЛР
Раздел 10	Основы безопасности сетевых технологий	10.1	Введение в Internet и Intranet. Способы нападения на сети и защита от межсетевого доступа. Особенности для различных уровней модели ISO/OSI.	ЛК, ЛР
		10.2	Технологии межсетевых экранов. Функции МЭ. Формирование политики межсетевого взаимодействия. Критерии оценки межсетевых экранов	ЛК, ЛР
		10.3	Построение защищенных виртуальных сетей VPN. Средства обеспечения безопасности VPN. ¶Защита на канальном и сеансовом уровнях. Протоколы PPTP, L2TP, SSL/TLS, SOCKS. ¶Защита на сетевом уровне. Протокол IPSEC.¶	ЛК, ЛР
		10.4	Безопасность удаленного доступа к локальной сети. Централизованный контроль. Управление доступом по схеме однократного входа с авторизацией.¶Технологии обнаружения атак. Классификация систем обнаружения и предотвращения атак (IDS/IPS). Угрозы и уязвимости беспроводных сетей.¶	ЛК, ЛР
Раздел 11	Организационно-правовое обеспечение защиты информации	11.1	Сущность и роль организационно-правовых аспектов информационной безопасности. Нормативная правовая база информационной безопасности. Закон РФ “Об информации, информационных технологиях и о защите информации”. ¶Виды и категории информации ограниченного доступа: государственная и другие виды тайн. Закон РФ “О государственной тайне”, “О коммерческой тайне”, “О персональных данных”, “О национальной платежной системе”, “О безопасности критической информационной инфраструктуры Российской Федерации”. Государственная система лицензирования и сертификации деятельности в области защиты информации. Указ Президента РФ “О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации”. Закон РФ “Об электронной цифровой подписи”. Уголовно-правовое регулирование защиты информации.¶	ЛК, ЛР
Раздел 12	Стандарты информационной безопасности	12.1	Исторический очерк развития зарубежных стандартов информационной безопасности. ГОСТ Р ИСО/МЭК 15408-2002, как аутентичный вариант общих критериев безопасности ИТ. Функциональные требования безопасности. Требования доверия к безопасности. Стандарты ISO/IEC 17799: 2002 (BS 7799:2000).	ЛК, ЛР
		12.2	Стандарты по менеджменту информационной безопасности ISO/IEC 27001-27040. Немецкие стандарты BSI. Стандарты SysTrust, SCORE, GIAC.¶Стандарты для беспроводных сетей.	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			Отечественные стандарты информационной безопасности. Стандарты обеспечение информационной безопасности организаций банковской системы Российской Федерации. ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2 – 2018.¶Стандарты информационной безопасности в Интернете (IETF, RFC).¶	
Раздел 13	Сертификация и аттестация в области информационной безопасности	13.1	Назначение и общая характеристика. Добровольная сертификация. Обязательное подтверждение соответствия. Декларирование соответствия. Обязательная сертификация.	ЛК, ЛР
		13.2	Проведение сертификационных испытаний: принципы проведения испытаний, документы сертификационных испытаний. Сертификация продукции, ввозимой из-за границы РФ. Сертификация на региональном и международном уровнях.	ЛК, ЛР

* - 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. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах – М.: Горячая линия-телеком, 2001г.,-148 с.

2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов, М.: Горячая линия – Телеком, 2006. - 544 с.

3. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учеб. пособие. – М.: Гелиос АРВ, 2006.- 528 стр.

4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебн. Пособие .- М.: ИД «ФОРУМ»: ИНФРА-М,2008.-416 с.

5. Moore T., Pym D., Ioannidis C., Economics of Information Security and Privacy, Springer, 2010, - 320 с.

6. Обеспечение информационной безопасности бизнеса, Под ред. Курило А.П., Альпина Паблишерз, 2011, - 392 с.

7. Бондарев В.В. Введение в информационную безопасность автоматизированных систем (2-е издание). – М.: МГТУ им. Н.Э. Баумана. 2018. – 252с

8. Организационно-правовое обеспечение информационной безопасности. под редакцией А.А. Александрова, М.П. Сычева – М.: МГТУ им. Н.Э. Баумана. 2018. – 292с.

9. Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры. – М.: Горячая линия – телеком, 2018. – 314с

Дополнительная литература:

1. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Ось-89, 1998.-336 с.

2. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю., Теоретические основы компьютерной безопасности, – М: Радио и связь, 2000. -192 с.

3. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. – М.: Гелиос АРБ, 2002. – 432 с.

4. Снытников А.А. Лицензирование и сертификация в области защиты информации. – М.: Гелиос АРВ, 2003.- 192 с.

5. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности: Учебное пособие. – М.: Гелиос АРВ, 2004.- 144 с.

6. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск.: БЕЛЛІТФОНД, 2005.-304 с.

7. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации: Учеб. пособие. – М.: Гелиос АРВ, 2005.- 224 с.

8. Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учеб. пособие. – М.: Гелиос АРВ, 2005.- 192 с.

9. Астахов А. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 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 «Основы информационной безопасности и киберустойчивости».

* - 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 информационной безопасности и киберустойчивости» 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.*