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:

02.04.02 ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

(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)

2023 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 02.04.02 «Фундаментальная информатика и информационные технологии» и изучается во 2 семестре 1 курса. Дисциплину реализует Департамент механики и процессов управления. Дисциплина состоит из 13 разделов и 40 тем и направлена на изучение фундаментальных основ информационной безопасности и защиты информации; 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 грамотности студентов по кибербезопасности.

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-5	Способен инсталлировать и сопровождать программное обеспечение информационных систем, осуществлять эффективное управление разработкой программных средств и проектов	ОПК-5.1 Знает порядок и особенности процесса инсталляции программного обеспечения информационных систем; ОПК-5.2 Умеет обеспечить сопровождение программного обеспечения информационных систем; ОПК-5.3 Владеет современными информационными технологиями и техническими средствами для осуществления эффективного управления разработкой программных средств и проектов;
ПК-2	Способен применять методы и технологии защиты информации для решения задач управления проектами в области информационных технологий в условиях неопределенностей и рисков информационных угроз	ПК-2.1 Знает современные теоретические и экспериментальные методы, применяемые для разработки технологий защиты информации и процессов профессиональной деятельности; ПК-2.2 Умеет определять эффективность применяемых методов для разработки технологий защиты информации и процессов профессиональной деятельности; ПК-2.3 Владеет современными теоретическими и экспериментальными методами для разработки технологий защиты информации и процессов профессиональной деятельности;

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-5	Способен инсталлировать и сопровождать программное обеспечение информационных систем, осуществлять эффективное управление разработкой программных средств и проектов	Информационные технологии в математическом моделировании; Технологии программирования;	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Научно-исследовательская работа; Преддипломная практика; Интеллектуальные информационные системы;
ПК-2	Способен применять методы и технологии защиты информации для решения задач управления проектами в области информационных технологий в условиях неопределенностей и рисков информационных угроз	Статистические методы анализа данных; Машинное обучение и анализ больших данных;	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Научно-исследовательская работа; Преддипломная практика; Криптология и практика шифрования; Разработка и безопасность веб-приложений; Защищенное программное обеспечение; *Искусственные нейронные сети (Обучение с подкреплением)***; *Artificial Neural Networks (Reinforcement Learning)***;

* - 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	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	ЛК, ЛР
		1.2	Объективная необходимость информационной безопасности и защиты информации.	ЛК, ЛР
		1.3	Определение информации. Документированная информация. Электронное сообщение. Активы. Ресурсы.	ЛК, ЛР
		1.4	Различные определения информационной безопасности, защиты информации, кибербезопасности, киберустойчивости. Современная постановка задачи защиты информации.	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.	ЛК, ЛР
		3.2	Положения Гражданского кодекса РФ по защите информации. Международное сотрудничество. Кодекс об административных правонарушениях. Уголовный кодекс и защита информации.	ЛК, ЛР
		3.3	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.	ЛК, ЛР
		4.2	Модель угроз и модель нарушителя информационной безопасности.	ЛК, ЛР
		4.3	Общая характеристика анализа, оценки и управления рисками. Шкалы. Оценка на основе выявления слабого звена. Оценка рисков на основе рассмотрения этапов вторжения.	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.	ЛК, ЛР
		5.2	Виды воздействия на информацию в ИС и АС. Угрозы безопасности АС и их классификация. Меры противодействия угрозам безопасности АС. Уязвимости АС.	ЛК, ЛР
		5.3	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	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			активная защита от утечки информации по техническим каналам. Определение, классификация и общая характеристика ТКУИ.	
		6.2	Визуальные и акустические каналы. Защита информации в телефонных каналах. Защита от побочных электромагнитных излучений и наводок (ПЭМИН). Технические закладки. Способы обнаружения ТКУИ.	ЛК, ЛР
		6.3	Способы и методы перекрытия ТКУИ. Требования к выбору и оборудованию помещений для АС обработки данных по условиям защиты от ТКУИ.	ЛК, ЛР
		6.4	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.	ЛК, ЛР
		7.2	Технические средства и системы охраны территории, зданий и помещений. Технические средства наблюдения и контроля за перемещением людей и предметов.	ЛК, ЛР
		7.3	Технические средства и системы опознавания людей. Технические средства и системы управления доступом на территорию, в здания и помещения, к средствам обработки и хранения информации.	ЛК, ЛР
		7.4	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.	ЛК, ЛР
		8.2	Способы разграничения доступа, методы и средства их реализации. Краткая характеристика современных средств разграничения доступа.	ЛК, ЛР
		8.3	Математические модели управления доступом к информации. Субъектно-объектная модель доступа. Политика безопасности и модель доступа. Электронные ключи.	ЛК, ЛР
		8.4	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. Основные каналы распространения вирусов и других вредоносных программ.	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	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			модели ISO/OSI.	
		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.	ЛК, ЛР
		10.4	Защита на сетевом уровне. Протокол IPSEC. Безопасность удаленного доступа к локальной сети. Централизованный контроль. Управление доступом по схеме однократного входа с авторизацией.	ЛК, ЛР
Раздел 11	Организационно-правовое обеспечение защиты информации.	11.1	Сущность и роль организационно-правовых аспектов информационной безопасности. Нормативная правовая база информационной безопасности.	ЛК, ЛР
		11.2	Уголовно-правовое регулирование защиты информации.	ЛК, ЛР
Раздел 12	Стандарты информационной безопасности.	12.1	Исторический очерк развития зарубежных стандартов информационной безопасности	ЛК, ЛР
		12.2	Стандарты для беспроводных сетей. Отечественные стандарты информационной безопасности.	ЛК, ЛР
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	

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
	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.

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. Снытников А.А. Лицензирование и сертификация в области защиты информации. – М.: Гелиос АРВ, 2003.- 192 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 «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**!

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 «Технологические угрозы и системы обеспечения 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:

Доцент		Варфоломеев Александр Алексеевич
Должность, БУП	*Подпись*	*Фамилия И.О.*