Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы»

Факультет искусственного интеллекта

(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/специальности)

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

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(наименование (профиль/специализация) ОП ВО)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Защита информации от утечки по техническим каналам» входит в программу бакалавриата «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» по направлению 10.03.01 «Информационная безопасность» и изучается в 6 семестре 3 курса. Дисциплину реализует Кафедра прикладного искусственного интеллекта. Дисциплина состоит из 1 раздела и 18 тем и направлена на изучение методов и средств предотвращения несанкционированного доступа к информации через технические каналы связи и оборудование. В рамках этого курса студенты знакомятся с различными видами технических каналов утечки информации, способами их обнаружения и нейтрализации, а также с техническими мерами защиты информации, такими как экранирование, фильтрация сигналов и использование специальных защитных устройств.

Целью освоения дисциплины является подготовка специалистов, способных выявлять и нейтрализовать технические каналы утечки информации, а также применять современные методы и средства защиты для обеспечения безопасности информационных систем и предотвращения несанкционированного доступа к конфиденциальным данным.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Защита информации от утечки по техническим каналам» 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 в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.2 Принимает участие в формировании политики информационной безопасности, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации на объекте защиты;
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2 Применяет средства технической защиты информации для решения задач профессиональной деятельности;
оОПК-2.1	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	пОПК-2.1.1 Знает возможные функциональные процессы объекта защиты и его информационных составляющих для выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба пОПК-2.1.2 Проводит анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба
оОПК-2.2	Способен проводить анализ функционального процесса объекта защиты и его	пОПК-2.2.1 Знает методы оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих для

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	повышения их устойчивости к деструктивным воздействиям на информационные ресурсы пОПК-2.2.2 Формирует предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы
оОПК-2.4	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	пОПК-2.4.1 Знает методы и средства проведения аудита защищенности объекта информатизации в соответствии с нормативными документами

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Защита информации от утечки по техническим каналам» 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 «Защита информации от утечки по техническим каналам».

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 применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Аппаратные средства вычислительной техники; Физические основы защиты информации;	Методы и средства криптографической защиты информации; Комплексное обеспечение защиты информации объекта информатизации; Технологическая практика;
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	Организационное и правовое обеспечение информационной безопасности;	Технологическая практика; Комплексное обеспечение защиты информации объекта информатизации;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
оОПК-2	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	Аппаратные средства вычислительной техники; Физические основы защиты информации; Организационное и правовое обеспечение информационной безопасности;	Анализ и управление рисками информационной безопасности; Программно-аппаратные средства защиты информации; Комплексное обеспечение защиты информации объекта информатизации; Технологическая практика; Аудит информационной безопасности;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Защита информации от утечки по техническим каналам» составляет «5» 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)**
			6
Контактная работа, ак.ч.	*78*		*78*
Лекции (**ЛК**)	39		39
Лабораторные работы (**ЛР**)	39		39
Практические/семинарские занятия (**СЗ**)	0		0
Самостоятельная работа обучающихся, ак.ч.	*66*		*66*
Контроль (экзамен/зачет с оценкой), ак.ч.	*36*		*36*
Общая трудоемкость дисциплины	**ак.ч.**	***180***	*180*
	зач.ед.	***5***	*5*

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	Защита информации от утечки по техническим каналам	1.1	Защищаемые объекты и их свойства	ЛК, ЛР
		1.2	Общие положения защиты информации техническими средствами	ЛК, ЛР
		1.3	Физические основы функционирования систем обработки и передачи информации	ЛК, ЛР
		1.4	Принципы и способы добывания информации	ЛК, ЛР
		1.5	Технические каналы утечки информации	ЛК, ЛР
		1.6	Методы и средства технической разведки	ЛК, ЛР
		1.7	Защита объектов от химической, радиационной и магнитометрической разведок	ЛК, ЛР
		1.8	Акустический канал утечки информации. Системы защиты от утечки информации по акустическому каналу	ЛК, ЛР
		1.9	Проводной канал утечки информации. Системы защиты от утечки информации по проводному каналу	ЛК, ЛР
		1.10	Вибрационный канал утечки информации. Системы защиты от утечки информации по вибрационному каналу	ЛК, ЛР
		1.11	Электромагнитный канал утечки информации. Системы защиты от утечки информации по электромагнитному каналу	ЛК, ЛР
		1.12	Телефонный канал утечки информации. Системы защиты от утечки информации по телефонному каналу	ЛК, ЛР
		1.13	Электросетевой канал утечки информации. Системы защиты от утечки информации по электросетевому каналу	ЛК, ЛР
		1.14	Оптический канал утечки информации. Системы защиты от утечки информации по оптическому каналу	ЛК, ЛР
		1.15	Защита информации техническими средствами в учреждениях и на предприятиях	ЛК, ЛР
		1.16	Поиск средств несанкционированного съема информации	ЛК, ЛР
		1.17	Моделирование объектов защиты и каналов утечки информации	ЛК, ЛР
		1.18	Контроль эффективности мер по защите информации техническими средствами	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	Лекционный класс для практической подготовки, проведения занятий лекционного типа, занятий	Комплект специализированной мебели: учебная доска; технические средства: Интерактивная панель 86 дюймов HUAWEI idea Hub S2 IHS2-86SA со встраиваемым OPS компьютером HUAWEI в комплекте с подвижной подставкой HUAWEI idea Hub White

	семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Rolling Stand _25, Двух объективная PTZ-видеокамера Nearity V520d, Системный блок CPU Intel Core I9-13900F/MSI PRO Z790-S Soc-1700 Intel Z790 / Samsung DDR5 16GB DIMM 5600MHz 2шт/ Samsung SSD 1Tb /Видеокарта RTX3090 2; Монитор LCD LG 27" 27UL500-W белый IPS 3840x2160 5ms 300cd 1000:1 (Mega DCR) DisplayPort P HDMIx2 Audioout, vesa. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/Office 365, Teams, Skype). Количество посадочных мест - 28.
Семинарская	Лаборатория радиоэлектроники для проведения лабораторных и практических занятий.	Комплект специализированной мебели: учебная доска; технические средства: Осциллограф Iwatsu ACK-7042, Прибор для измерения АЧХ Х1-53, Осциллограф МНИПИ С1-151, Источник питания СИП-301, Источник питания ВИП-010, Генератор импульсов Г5-54, Генератор сигналов НЧ МНИПИ Г3-131, Вольтметр универсальный В7-21, Генератор сигналов ВЧ Г4-116, Вольтметр В7-35, Измеритель индуктивности Е7-11, Прибор для измерения АЧХ Х1-48, Генератор-частотомер Актаком АНР-1001, Генератор сигналов Г3-20, Генератор сигналов НЧ Г3-118, Источник питания ТЕС 20, Источник питания ТЕС 21, Источник питания ТЕС 9, Источник питания ТЕС 13, Источник питания ТЕС 18, Частотомер Ч3-34А, Частотомер Ч3-54, Анализатор спектра С4-25, Блок СВЧ С4-24, Генератор сигналов ВЧ Г4-102А, Синтезатор частоты Ч6-31, Блок генераторный к Х1-53, Блок ГКЧ Х1-46, Мост емкостей Е8-2, Измеритель нелинейных искажений С6-1А, Лабораторный стенд СПЭ-8, Лабораторный стенд ЛРС-2, Усилитель измерительный НЧ У4-28, Милливольтметр В3-43. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т.ч. MS Office/ Office 365, Teams, Skype), Borland Developer Studio 2006, MATLAB R2008b, Notepad++, Acrobat Reader DC, Anaconda 5 (Python 3).
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.	Компьютерный класс для практической подготовки, проведения занятий практико-лабораторного характера, самостоятельной работы, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Комплект специализированной мебели; учебная доска; технические средства: Моноблок HP ProOne 440 Intel I5 10500T/8 GB/256 GB/audio, монитор 24"; Мультимедиа проектор Casio XJ-V100W; Экран, моторизованный Digis Electra 200*150 Dsem-4303 Программное обеспечение: Продукты Microsoft (MS Windows, MS Office) – подписка Enrollment for Education Solution (EES) №56278518 от 23.04.2019
		Компьютерный класс - учебная аудитория для практической подготовки, лабораторно-практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также самостоятельной работы Комплект специализированной мебели; (в т.ч. электронная доска); мультимедийный проектор BenqMP610; экран моторизованный Sharp 228*300; доска аудиторная поворотная; Комплект ПК iRU Corp 317 TWR i7 10700/16GB/ SSD240GB/2TB 7.2K/ GTX1660S-6GB /WIN10PRO64/ BLACK + Комплект Logitech Desktop MK120, (Keybord&mouse), USB, [920-002561] + Монитор HP P27h G4 (7VH95AA#ABB) (УФ-000000000059453)-5шт., Компьютер Pirit Doctrin4шт.,

		ПО для ЭВМ LiraServis Academic Set 2021 Состав пакета ACADEMIC SET: программный комплекс "ЛИРА-САПР FULL". программный комплекс "МОНОМАХ-САПР PRO". программный комплекс "ЭСПРИ.

* - аудитория для самостоятельной работы обучающихся указывается **ОБЯЗАТЕЛЬНО**!

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: Учебник для вузов, под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО "Издательство Машиностроение", 2009. - 508 с.

2. Нестеров С.А. Информационная безопасность и защита информации: Учебное пособие. - СПб.: Изд-во Политехн. ун-та, 2009. - 126 с.

3. Сидорин Ю.С. Технические средства защиты информации: Учебное пособие. - СПб.: СПбГПУ, 2005. - 141 с.

4. Царегородцев А.В. Техническая защита информации: учебное пособие. – М.: Финансовый университет, 2013. – 276 с.

5. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. - М: ФОРУМ, 2013 г., 592 с.

Дополнительная литература:

1. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Изд. Гелиос АРВ, 2007.

2. Железняк В.К. Защита информации от утечки по техническим каналам. – СПб.: Изд. ГУАП, 2006.

3. Информационная безопасность и защита информации: Учебное пособие. - Ростов-на-Дону: Ростовский юридический институт МВД России, 2004. - 82 с.

4. Камышев Э.Н. Информационная безопасность и защита информации: Учебное пособие. - Томск: ТПУ, 2009. - 95 с.

5. Кондратьев А.В. Техническая защита информации. Практика работ по оценке основных каналов утечки. – М.: Горячая линия – Телеком, 2016.

6. Курило А.П., Зефиров С.Л., Голованов В.Б. Аудит информационной безопасности. – М.: Изд. БДЦ-Пресс, 2006.

7. Меньшаков Ю.К. Виды и средства иностранных технических разведок: учеб. пособие. Под ред. М.П. Сычева. – М.: Изд.- во МГТУ им. Н.Э. Баумана, 2009. – 656 с.

8. Парошин А.А. Нормативно-правовые аспекты защиты информации: Учебное пособие. - Владивосток: Изд-во Дальневост. федер. ун-та, 2010. - 116 с.

9. Технологии и принципы защиты информации. Программа дисциплины. - М.: МГУ, 2004.

- Терехов А.В., Чернышов В.Н., Селезнев А.В., Рак И.П. Защита компьютерной информации: Учебное пособие. - Тамбов: Изд-во ТГТУ, 2003. - 80 с.

10. Торокин А.А. Инженерно-техническая защита информации: учебное пособие. – М.: Изд. Гелиос АРВ, 2005.

11. Хорев А.А. Техническая защита информации: учеб. Пособие для студентов вузов. В 3 т. Т.1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.: ил.

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 «Защита информации от утечки по техническим каналам».

* - 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 «Защита информации от утечки по техническим каналам» представлены в Приложении к настоящей Рабочей программе дисциплины.

* - ОМ и БРС формируются на основании требований соответствующего локального нормативного акта РУДН.