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 информационной безопасности . 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 обучающиеся 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;
пОПК-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;
пОПК-2.2	Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	пОПК-2.2.1 Знает методы оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих для 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;
пОПК-2.4	Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	пОПК-2.4.2 Проводит аудит защищенности объекта информатизации в соответствии с нормативными документами;
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач	ОПК-9.2 Применяет средства технической защиты информации для решения задач профессиональной деятельности;

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	профессиональной деятельности	

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;
пОПК-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	Аппаратные средства вычислительной техники; Физические основы защиты информации;	Технологическая практика; Анализ и управление рисками информационной безопасности; Программно-аппаратные средства защиты информации; Комплексное обеспечение защиты информации объекта информатизации;
пОПК-2.2	Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы		Комплексное обеспечение защиты информации объекта информатизации;
пОПК-2.4	Способен проводить аудит защищенности объекта	Организационное и правовое обеспечение информационной безопасности;	Аудит информационной безопасности;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
	информатизации в соответствии с нормативными документами		

* - 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 «6» 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.	*102*		*102*
Контроль (экзамен/зачет с оценкой), ак.ч.	*36*		*36*
Общая трудоемкость дисциплины ак.ч.	**ак.ч.**	**216**	**216**
	зач.ед.	**6**	**6**

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

*Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы**

Номер раздела	Наименование раздела дисциплины	Наименование 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	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническими средствами мультимедиа презентаций.	Персональный компьютер или моноблок с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска.
Лаборатория	Аудитория для проведения лабораторных работ, индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и оборудованием.	Персональные компьютеры или моноблоки с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска. Программное обеспечение: среда виртуализации Oracle VM VirtualBox (свободно-распространяемое ПО), операционная система Debian Linux (свободно-распространяемое ПО), интерпретатор Python (свободно-распространяемое ПО), свободно-распространяемые программные пакеты симуляции физических атак (например, SeseLab и GRFICSv3 (свободно-распространяемое ПО)).
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве 25 шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	Персональные компьютеры или моноблоки с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска. Программное обеспечение: среда виртуализации Oracle VM VirtualBox (свободно-распространяемое ПО), операционная система Debian Linux (свободно-распространяемое ПО), интерпретатор Python (свободно-распространяемое ПО), свободно-распространяемые программные пакеты симуляции физических атак (например, SeseLab и GRFICSv3 (свободно-распространяемое ПО)).
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.	Персональный компьютер или моноблок с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет).

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Помазанов, А. В. Защита информации от утечки по техническим каналам : учебное пособие / А. В. Помазанов ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2024. - 134 с. – ISBN 978-5-9275-4851-4. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2220025 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

2. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки

информации : учебное пособие : [16+] / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет им. А. А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=694670 (дата обращения: 26.03.2026). – Библиогр.: с. 117-118. – ISBN 978-5-4499-3327-0. – DOI 10.23681/694670. – Текст : электронный.

3. Зайцев, А. П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. - Москва : Гор. линия-Телеком, 2012. - 442с.; - (Уч. для вузов). ISBN 978-5-9912-0233-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/390284 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

Дополнительная литература:

1. Техническая защита информации : практикум / сост. А. С. Кравченко, В. А. Мельник, С. Л. Сахаров ; ФКОУ ВО Воронежский институт ФСИН России. - Иваново : Издательско-полиграфический комплекс «ПресСто», 2023. - 80 с. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2158325 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

2. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]. - Саров : РФЯЦ-ВНИИЭФ, 2019. - 267 с. - ISBN 978-5-9515-0426-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1230831 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

3. Сидак, А. А. Методы и средства защиты акустической речевой информации от утечки по техническим каналам : лабораторный практикум : [16+] / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет. – Москва : Директ-Медиа, 2023. – 92 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=699044 (дата обращения: 26.03.2026). – Библиогр. в кн. – ISBN 978-5-4499-3603-5. – DOI 10.23681/699044. – Текст : электронный.

4. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам: Справочное пособие / Бузов Г.А. - Москва :Гор. линия-Телеком, 2015. - 586 с. ISBN 978-5-9912-0424-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/895240 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

5. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 256 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1850081 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

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 https://mega.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 «Знаниум» https://znanium.ru/
2. Базы данных и поисковые системы
   - Sage https://journals.sagepub.com/
   - Springer Nature Link https://link.springer.com/
   - Wiley Journal Database https://onlinelibrary.wiley.com/
   - Наукометрическая база данных Lens.org https://www.lens.org

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**!

РАЗРАБОТЧИКИ:

Заведующий кафедрой информационной безопасности		Царегородцев А.В.
Должность	*Подпись*	*Фамилия И.О*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой информационной безопасности		Царегородцев А.В.
Должность	*Подпись*	*Фамилия И.О*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой информационной безопасности		Царегородцев А.В.
Должность	*Подпись*	*Фамилия И.О*