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)

2026 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 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-14	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	ОПК-14.1 Знает возможные функциональные процессы объекта защиты и его информационных составляющих для выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба; ОПК-14.2 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;
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;

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	Физические основы защиты информации;	Технологическая практика; Методы и средства криптографической защиты информации;
ОПК-14	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;

* - 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.**	***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		Содержание темы	Вид учебной работы*
Раздел 1	Защита информации от утечки по техническим каналам	1.1	Защищаемые объекты и их свойства	Цели и задачи технической защиты информации. Предмет, цели, задачи и содержание курса в целом, его роль и место в подготовке специалистов по комплексной защите информации. Место технической защиты информации в системе комплексной защиты информации. Виды информации, защищаемой техническими средствами. Системный подход при решении задач технической защиты информации. Основные признаки аналоговых и дискретных электрических сигналов, средств связи, лазерных излучений. Демаскирующие признаки объектов защиты. Видовые, сигнальные и вещественные демаскирующие признаки. Информативность признаков. Особенности видовых признаков в видимом, ИК и радиодиапазонах электромагнитных волн.	ЛК, ЛР
		1.2	Общие положения защиты информации техническими средствами	Задачи и требования к способам и средствам защиты конфиденциальной информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты. Сущность организационных и технических мер защиты.	ЛК, ЛР
		1.3	Физические основы функционирования систем обработки и передачи информации	Физические эффекты в технических системах. Закономерности технической реализации физических эффектов. Конструктивно-технологические закономерности. Основы функционирования электромагнитных каналов связи. Свойства физических полей, электрических сигналов и материальных тел как носителей информации.	ЛК, ЛР
		1.4	Принципы и способы добывания информации	Способы доступа к источникам конфиденциальной информации. Наблюдение, перехват, подслушивание. Этапы добывания и обработки информации. Текущие и эталонные первичные и вторичные признаковые структуры. Принципы идентификации и интерпретации признаков обнаружения и распознавания объектов, измерение их характеристик.	ЛК, ЛР
		1.5	Технические каналы утечки информации	Условия и особенности утечки информации. Структура канала утечки. Виды каналов утечки. Условия образования каналов	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				утечки. Характеристики каналов утечки информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Акустические каналы утечки информации.	
		1.6	Методы и средства технической разведки	Классификация технических средств разведки по видам их носителей. Методы и средства технической разведки. Потенциальные каналы утечки информации на предприятиях. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Общая характеристика радиоэлектронной разведки, ее особенности. Средства дистанционного съема информации. Принципы миниатюризации и камуфлирования средств разведки под бытовые приборы. Принципы комплексного использования технических средств разведки различных видов.	ЛК, ЛР
		1.7	Защита объектов от химической, радиационной и магнитометрической разведок	Способы и средства защиты объектов от химической и радиационной разведок. Способы защиты химического и радиационного оборудования, производственных отходов, сточных вод и газообразных выбросов, сырья и готовой продукции. Способы защиты металлических объектов большой массы, установленных на воздушных носителях, от средств магнитометрической разведки. Методические рекомендации по оценке эффективности защиты от радиационной, химической и магнитометрической разведок.	ЛК, ЛР
		1.8	Акустический канал утечки информации. Системы защиты от утечки информации по акустическому каналу	Технические средства акустической разведки: принцип действия, основные функции. Непосредственное подслушивание звуковой информации. Прослушивание информации от структурной волны. Прослушивание информации направленными микрофонами. Недостатки направленных микрофонов. Деконспирационные признаки. Система защиты от утечки по акустическому каналу. Схема пассивного акустоэлектрического канала утечки информации. Схема активного акустоэлектрического канала утечки информации.	ЛК, ЛР
		1.9	Проводной канал утечки информации. Системы защиты от утечки информации по проводному каналу	Упрощенный принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны.	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				Деконспирационные признаки. Системы защиты от диктофонов.	
		1.10	Вибрационный канал утечки информации. Системы защиты от утечки информации по вибрационному каналу	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Деконспирационные признаки. Системы защиты информации от утечки по вибрационному каналу.	ЛК, ЛР
		1.11	Электромагнитный канал утечки информации. Системы защиты от утечки информации по электромагнитному каналу	Общая характеристика радиоэлектронной разведки, ее особенности. Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры: утечка информации от мощной офисной аппаратуры, утечка информации от вспомогательной аппаратуры и кабелей проходящих через помещение. Прослушивание информации от внедрённых радиозакладок: основные характеристики радиозакаладок, основные элементы радиозакладок. Прослушивание информации от пассивных закладок. Приемники информации с радиозакладок. Деконспирационные признаки. Системы защиты от утечки по электромагнитному каналу: методы пассивной и активной защиты. Технические средства для поиска работающих радиозакладок. Поиск радиозакладок нелинейными радиолокатарами.	ЛК, ЛР
		1.12	Телефонный канал утечки информации. Системы защиты от утечки информации по телефонному каналу	Контактный и бесконтактный метод съема информации за счет непосредственного подключения аппаратуры к телефонной линии: непосредственное подключение к телефонной линии, применение трансформаторов, применение индуктивных датчиков, применение преобразователей Холла. Использование микрофона телефонного аппарата при положенной телефонной трубке: общий принцип телефонного аппарата, доработка телефонного аппарата с целью использования его микрофона, беззаходовый НСИ. Применение диктофонов. Телефонные ретрансляторы. Утечка информации по сотовым цепям связи. Деконспирационные признаки. Устройства защиты от утечки информации по телефонному каналу: обнаружение устройств, потребляющих ток из телефонной сети, устройства, предотвращающие использование микрофона телефонного аппарата, устройства, предотвращающие включение магнитофона, включающегося при подъеме трубки,	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				многофункциональные устройства индивидуальной защиты телефонных линий. Защита от НСИ в радиотелефонных каналах. Устройства уничтожения закладок.	
		1.13	Электросетевой канал утечки информации. Системы защиты от утечки информации по электросетевому каналу	Особенности передачи сигнала по электросетевому каналу. Низкочастотное устройство съема информации. Высокочастотное устройство съёма информации. Деконспирационные признаки. Системы защиты от утечки по электросетевому каналу.	ЛК, ЛР
		1.14	Оптический канал утечки информации. Системы защиты от утечки информации по оптическому каналу	Приборы ночного видения. Телевизионные системы наблюдения. Системы защиты от утечки по оптическому каналу.	ЛК, ЛР
		1.15	Защита информации техническими средствами в учреждениях и на предприятиях	Организация работ по инженерно-технической защите на предприятиях и в учреждениях государственных и коммерческих структур. Основные руководящие документы по защите предприятий и учреждений от технической разведки. Аналитическое обоснование необходимости создания подсистемы системы защиты информации от ее утечки по техническим каналам. Проектирование системы технической защиты информации (СТЗИ) объекта информатизации. Нормы допустимых уровней излучений. Аттестация выделенных помещений. Порядок ввода объекта информатизации и СТЗИ в эксплуатацию. Особенности защиты информации о продукции на различных этапах ее жизненного цикла.	ЛК, ЛР
		1.16	Поиск средств несанкционированного съема информации	Организационные и технические мероприятия по защите информации в учреждениях и на предприятиях. Поиск СНСИ и пути подавления. Методика комплексной проверки выделенных помещений.	ЛК, ЛР
		1.17	Моделирование объектов защиты и каналов утечки информации	Структурные, функциональные и информационные модели объектов защиты и каналов утечки. Принципы построения комплексных моделей объектов защиты и каналов утечки. Подходы к оценке угрозы каналов утечки и безопасности конфиденциальной информации.	ЛК, ЛР
		1.18	Контроль эффективности мер по защите информации техническими средствами	Модели систем защиты и показатели эффективности. Стоимость защиты. Рекомендации по выбору рациональных вариантов защиты информации и соответствующих технических средств. Технический контроль эффективности	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				принимаемых мер защиты. Назначение, содержание, вид и методы технического контроля. Основные средства технического контроля. Оценка возможностей по перехвату побочных электромагнитных излучений от средств вычислительной техники техническими средствам разведки. Пассивные средства защиты объектов информатизации. Активные средства защиты объектов информатизации.	

* - 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), программные пакеты симуляции физических атак 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), программные пакеты симуляции физических атак SeseLab и GRFICSv3 (свободно-распространяемое ПО).
Семинарская	Аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели 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.
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**!

РАЗРАБОТЧИК:

Заведующий кафедрой информационной безопасности		Царегородцев Анатолий Валерьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой информационной безопасности		Царегородцев Анатолий Валерьевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой информационной безопасности		Царегородцев Анатолий Валерьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*