

УДК 004.056

Г.П. ГАВДАН

Национальный исследовательский ядерный университет «МИФИ», Москва

ПРОБЛЕМЫ И НАПРАВЛЕНИЯ РАЗВИТИЯ СИСТЕМ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Стремительное развитие речевых технологий на основе искусственного интеллекта (ИИ), включая распознавание, синтез и анализ речи, создает новые киберугрозы и вызовы в области защиты информации (ЗИ). В работе систематизированы ключевые проблемы защиты речевой информации и перспективные направления развития защитных механизмов.

Введение

Широкое внедрение искусственного интеллекта в речевые технологии кардинально трансформирует человеко-машинное взаимодействие, стремясь сделать его не только точным, но и контекстуально осмысленным. Однако эта эволюция создает новые векторы для кибератак, предоставляя злоумышленникам мощные инструменты на основе тех же технологий ИИ. В связи с этим, задача обеспечения безопасности речевых данных и систем их обработки приобретает критическую актуальность, требуя опережающего развития методов и средств защиты информации.

Ключевые проблемы защиты речевой информации

Анализ современных исследований [1–3] позволяет выделить следующие системные проблемы:

1. *Уязвимости моделей машинного обучения:* речевые системы на основе ИИ уязвимы к атакам.
2. *Риски конфиденциальности и этики:* сбор и обработка биометрических голосовых данных создают риски слежения.
3. *Зависимость от импортных технологий:* использование зарубежных платформ и фреймворков создает риски к защите данных.
4. *Высокие требования к вычислительным ресурсам:* реализация сложных алгоритмов защиты и шифрования речи в реальном времени.

Перспективные направления развития защитных механизмов

Для противодействия указанным угрозам развиваются следующие технологические направления, сущность и примеры которых систематизированы в табл. 1.

Таблица 1. Направления развития систем ЗИ в речевых технологиях

№	Направления развития	Сущность и примеры защитных механизмов
1	Упреждающий анализ угроз	Глубокий семантический анализ для выявления скрытых угроз; прогнозирование моделей поведения нарушителей; обнаружение аномалий в речевых потоках.
2	Активная защита на основе Generative AI	Генерация защищенных речевых сигналов, устойчивых к искажению; создание систем для проверки подлинности голоса (AI-верификаторы); разработка методов цифрового водяного знака для синтезированной речи.
3	Мультимодальная аутентификация	Комбинирование голосовой биометрии с анализом лицевых образов и поведенческих паттернов для повышения надежности идентификации.
4	Конфиденциальность данных	Применение методов деидентификации голоса; использование гомоморфного шифрования для обработки данных без их расшифровки; внедрение блокчейн-технологий для обеспечения неизменности голосовых логов.
5	Обеспечение доступности и целостности	Разработка систем речевого оповещения, устойчивых к шумовым и помеховым воздействиям; создание инструментов для лиц с нарушениями речи.

Проведенный анализ демонстрирует, что развитие речевых технологий неразрывно связано с эскалацией киберугроз.

Заключение

Дальнейшие исследования необходимо сконцентрировать на создании отечественных защищенных речевых платформ, способных функционировать в условиях импортозамещения. Для обеспечения безопасности необходима комплексная стратегия, включающая:

1. разработку адаптивных алгоритмов защиты;
2. внедрение архитектур безопасности «по умолчанию»;
3. создание нормативно-правовой базы (НПБ), регламентирующей сбор, обработку и использование биометрических голосовых данных.

Список литературы

1. Перспективные направления применения технологий искусственного интеллекта при защите информации / Р.В. Мещеряков, С.Ю. Мельников, В.А. Пересыпкин, А.А. Хорев // Вопросы кибербезопасности. – 2024. – № 4(62). – С. 2–12. – DOI 10.21681/2311-3456-2024-4-02-12. – EDN GJWQWP (дата обращения: 25.09.2025).
2. Дураковский, А.П. Эволюция и направления развития технологий маскирования конфиденциальных речевых сообщений / А.П. Дураковский, С.В. Дворянкин, Н.С. Дворянкин // Вопросы кибербезопасности. – 2024. – № 5(63). – С. 58–66. – DOI 10.21681/2311-3456-2024-5-58-66. – EDN АОВХХМ (дата обращения: 29.09.2025).
3. Дворянкин, С.В. Лабораторный комплекс «Образный анализ и защита речевой информации в интеллектуальных системах» / С.В. Дворянкин // Приборы и системы. Управление, контроль, диагностика. – 2023. – № 6. – С. 66–72. – DOI 10.25791/prigor.6.2023.1419. – EDN IMXOAK (дата обращения: 29.09.2025).