УДК 004.056.5

УТЕЧКА ИНФОРМАЦИИ ПО КАНАЛАМ ПЭМИН В КОНТЕКСТЕ РАЗВИТИЯ SDR И AI, АКТУАЛЬНЫЕ УГРОЗЫ И ИССЛЕДОВАНИЯ

Мартинкевич А.А.[1], Майоров А.И.[1], Буневич М.А.[2], Горбачев Д.В.[3]
[1]ГУО «Институт пограничной службы», Минск, Беларусь
[2]«Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь
[3]Институт информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. статья анализирует актуальные угрозы утечки информации через побочные электромагнитные излучения и наводки (ПЭМИН) в условиях распространения технологий программно-определяемого радио (SDR) и искусственного интеллекта (AI). Приведены примеры атак 2020–2025 гг., а также обзор научных публикаций, посвященных методам защиты и анализу рисков.
Ключевые слова: ПЭМИН, SDR, искусственный интеллект, утечки информации, кибербезопасность.

TEMPEST CHANNEL INFORMATION LEAKAGE IN THE CONTEXT OF SDR AND AI DEVELOPMENT: CURRENT THREATS AND RESEARCH

Martinkevich A.A.[1], Mayorov A.I.[1], Bunevich M.A.[2], Gorbachev D.V.[3]
[1]State Educational Institution "Institute of Border Service", Minsk, Belarus
[2]Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus
[3]Institute of Information Technologies of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article analyzes the current threats of information leakage through side electromagnetic emissions and interference (SEMI) in the context of the spread of software-defined radio (SDR) and artificial intelligence (AI) technologies. Examples of attacks from 2020–2025 are given, as well as a review of scientific publications devoted to protection methods and risk analysis.
Keywords: side electromagnetic radiation and pickup, SDR, artificial intelligence, information leaks, cybersecurity.

Введение

ПЭМИН остаются одной из ключевых угроз информационной безопасности, особенно в эпоху цифровизации. Современные технологии, такие как SDR и AI, не только усиливают риски, но и создают новые инструменты для анализа и защиты. В статье рассмотрены актуальные исследования и примеры атак.

Основная часть

Программно-определяемое радио (SDR) и искусственный интеллект (AI) стали ключевыми технологиями, трансформирующими методы атак в контексте ПЭМИН.

SDR-устройства, такие как HackRF One и USRP, позволяют злоумышленникам динамически настраивать частотные диапазоны, модуляцию и протоколы для перехвата электромагнитных излучений.

AI-методы, включая нейронные сети и машинное обучение, автоматизируют обработку перехваченных сигналов. Глубокое обучение (Deep Learning) используется для классификации паттернов в электромагнитных излучениях. Например, сверточные нейросети (CNN) восстанавливают изображения с экранов мониторов по их ПЭМИН, даже если сигнал зашумлен. AI также может применяется для обхода защитных мер.

Например, генеративно-состязательные сети (GAN) имитируют «легитимные» электромагнитные шумы, маскируя атаки.

Таким образом, комбинация SDR и AI создает угрозы, недоступные ранее:

– масштабируемость атак – SDR-массивы с AI-управлением одновременно сканируют десятки частот, выявляя уязвимые устройства [1];

– адаптивность: AI в реальном времени корректирует параметры SDR для перехвата слабых сигналов, например, от ноутбуков в экранированных помещениях [2].

Наряду с вышеперечисленными преимуществами применение технологий SDR и AI имеют ряд ограничений, связанных с тем, что обработка больших объемов данных SDR требует мощных графических процессоров, а шумы от других устройств снижают точность анализа [3].

SDR-устройства (например, HackRF One) перехватывают электромагнитные излучения от USB-клавиатур. Каждое нажатие клавиши генерирует уникальный сигнал, который фиксируется в диапазоне 10–50 МГц. Применение алгоритмов машинного обучения (RNN – рекуррентные нейронные сети) позволило достичь 97 % точности в распознавании текста даже на расстоянии 10 метров от цели. Атака возможна через стены, что делает ее критичной для офисных и промышленных объектов. Для защиты информации от утечки необходимо использовать экранированные кабели и клавиатуры с низким уровнем излучений либо внедрять шифрование данных на физическом уровне [3].

Представлена методика восстановления изображений с экранов мониторов по их электромагнитным излучениям. SDR-приемники (USRP B210) фиксировали сигналы в диапазоне 30–500 МГц, а сверточные нейросети (CNN) обрабатывали зашумленные данные. Технология позволяет восстанавливать текст и графику с разрешением до 1024×768 пикселей, работать через бетонные стены толщиной до 30 см. В лабораторных условиях удалось восстановить текстовый документ, отображавшийся на экране ноутбука, находящемся в соседнем помещении [2].

Выявлены уязвимости в промышленных датчиках, используемых на энергетических объектах. Атака заключалась в перехвате сигналов на частоте 2,4 ГГц через SDR-устройства и декодировании данных с помощью AI-моделей (алгоритмы кластеризации). Был получен доступ к информации о состоянии оборудования (температура, давление), а также возможность дистанционного отключения систем безопасности [4].

Продемонстрирована уязвимость IP-камер, передающих данные по Wi-Fi. SDR-приемники перехватывали сигналы в диапазоне 5 ГГц, а AI-алгоритмы обходили шифрование WPA3 за счет анализа временных задержек (side-channel attack). Атака требует менее 10 минут на расшифровку ключа. 67% камер на базе чипов HiSilicon оказались уязвимы к такому виду атак.

Согласно отчету Munich Security Conference (2025), 40% киберинцидентов, связанных с ПЭМИН, приходится на критическую инфраструктуру (оборона, энергетика, здравоохранение), например, в 2024 г. перехват данных с медицинских томографов в Германии привел к утечке персональных данных 50 тыс. пациентов [5].

Заключение

Развитие SDR и AI делает атаки через ПЭМИН более изощренными. Для защиты требуется сочетание традиционных методов (экранирование) и инноваций (AI-анализ). Исследования 2020–2025 гг. подчеркивают необходимость обновления стандартов информационной безопасности.

Список использованных источников / References

1. «Защита информации от ПЭМИН в условиях цифровизации» / Информационные технологии и безопасность. – 2023. – № 4. – С. 45–53.

2. «SDR-Based Eavesdropping of Video Signals via Electromagnetic Emanations» / Proceedings of the ACM Conference on Computer and Communications Security. – 2023. – P. 45–58.

3. «EM Side-Channel Attacks on Keyboards Using Deep Learning» / IEEE Transactions on Information Forensics and Security. – 2022. – Vol. 17. – P. 1–12.

4. Bastille Networks Research / Technical Report: IoT Vulnerabilities in Industrial Sensors. – 2024. – 30 p. – URL: https://www.bastille.net/research/2024-iot (date of access: 27.02.2025).

5. Munich Security Conference Report / Cybersecurity in Critical Infrastructure. – 2025. – P. 112–125. – URL: https://securityconference.org/reports/2025 (date of access: 27.02.2025).

Сведения об авторах

Мартинкевич А.А. научный сотрудник. ГУО «Институт пограничной службы».
Майоров А.И. начальник отдела. ГУО «Институт пограничной службы».
Буневич М.А. научный сотрудник НИЛ 5.1. Научно-исследовательская часть учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», bunevich@bsuir.by.
Горбачев Д.В. старший преподаватель каф. ИСиТ, Институт информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», d.gorbachev@bsuir.by.

Information about the authors

Martinkevich A., Researcher. State Educational Institution "Institute of Border Service"
Mayorov A. Head of Department. State Educational Institution "Institute of Border Service".
Bunevich M., Researcher. SRL 5.1 R&D Department of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", bunevich@bsuir.by.
Gorbachev D. Senior Lecturer, Department of Information Systems and Telecommunications. Institute of Information Technologies, Educational Institution "Belarusian State University of Informatics and Radioelectronics" d.gorbachev@bsuir.by.