ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 621.3

ЧТО ТАКОЕ АППАРАТНЫЙ ХАКИНГ И КАК ЭЛЕКТРИЧЕСТВО ВЫДАЕТ НАШИ СЕКРЕТЫ

Рудич Ярослав Юрьевич,
студент 4 курса, кафедры ИУ1
«Система управления летательными аппаратами»,
МГТУ им. Н.Э. Баумана,
РФ, г. Москва,
yaroslavrudich@mail.ru

Шпынкова Виктория Дмитриевна,
студентка 4 курса, кафедры ИУ1
«Система управления летательными аппаратами»,
МГТУ им. Н.Э. Баумана,
РФ, г. Москва,
shpynkova.viktoria@mail.ru

Аннотация

В кибербезопасности чаще всего говорят о вирусах и взломе программ. Но есть другой, менее известный способ атаки — через «железо» (аппаратуру). В этой статье рассказано, как хакеры могут вмешиваться в работу устройств: ловить электромагнитные сигналы от проводов, встраивать внутрь техники вредоносные чипы или ломать оборудование скачками напряжения. Также объясняется, как от этого защищаться.

Ключевые слова: аппаратный хакинг, побочные каналы утечки, электромагнитное излучение, внедрение ошибок, кибербезопасность.

WHAT IS HARDWARE HACKING AND HOW ELECTRICITY GIVES AWAY OUR SECRETS

Rudich Yaroslav Yurievich
4th year student, Departments of IU1
«Aircraft control system»,
Bauman Moscow State Technical University,
Russian Federation, Moscow,
yaroslavrudich@mail.ru

Shpynkova Victoria Dmitrievna
4th year student, Departments of IU1
«Aircraft control system»,
Bauman Moscow State Technical University,

Russian Federation, Moscow,
shpynkova.viktoria@mail.ru

ABSTRACT

In cybersecurity, viruses and software hacking are most often talked about. But there is another, less well—known method of attack - through hardware. This article describes how hackers can interfere with the operation of devices: catch electromagnetic signals from wires, embed malicious chips inside equipment, or break equipment with power surges. It also explains how to protect yourself from this.

Keywords: hardware hacking, side leakage channels, electromagnetic radiation, error injection, cybersecurity.

Когда мы слышим о хакерах, обычно представляем программиста, который взламывает серверы через интернет. Но есть и другой уровень угрозы — аппаратный. Злоумышленник может вмешаться в работу электроники напрямую через провода. Например: перехватить данные по наводке на кабели, встроить в устройство «жучок» или вывести его из строя мощным электрическим импульсом [1].

Любая электроника работает по законам физики. Ток в проводах создает магнитное поле. Любое вычисление потребляет энергию. Микросхемы чувствительны к перепадам напряжения. Хакеры используют эти особенности, чтобы украсть данные или нарушить работу системы [2]. Цель статьи — объяснить, как работают такие атаки и как от них защититься.

1. Перехват данных через электромагнитные излучения

1.1. Что такое side-channel (побочный канал) атаки

Побочные каналы — это физические эффекты, которые возникают при работе устройства. Например, когда процессор выполняет сложные расчеты, он начинает потреблять больше электричества или создавать характерные радиоволны. По этим признакам можно понять, какие данные он обрабатывает, и даже восстановить ключи шифрования.

Особенно опасны электромагнитные атаки. Хакеру даже не нужно прикасаться к устройству. Достаточно поднести специальный датчик. При переключении транзисторов внутри микросхем возникают токи, которые создают излучение. Это излучение выдает информацию о том, какие данные обрабатываются.

1.2. Как это работает на практике

В 1985 году голландский инженер Вим ван Эк доказал, что можно восстановить картинку с монитора, поймав его излучение через стену. Сейчас возможности хакеров стали шире. Например, они могут перехватывать сигналы от USB-клавиатуры. Каждое нажатие клавиши создает всплеск тока, и по этим всплескам можно определить, какие клавиши были нажаты, включая пароли [2].

2. Внедрение вредоносных компонентов в устройства

2.1. Аппаратные закладки («жучки»)

Иногда хакеры не ловят сигнал, а заранее внедряют внутрь техники вредоносные детали. Самый известный пример — поддельные USB-кабели. Внутри такого кабеля спрятан микроконтроллер. Когда вы подключаете его к компьютеру, он «говорит» компьютеру, что это клавиатура, и начинает вводить вредоносные команды.

Еще более сложный метод — чип-трекинг. На плату устройства впаивают микроскопический чип. Он может скрытно передавать данные или следить за работой. Найти такую закладку очень сложно, потому что устройство работает нормально.

2.2. Как обнаружить закладку

Чтобы найти вредоносный чип, нужно проверять устройство под микроскопом, делать рентген, следить за аномалиями в энергопотреблении. Для особо важных систем контролируют цепочку поставок: от завода до установки.

3. Атаки через электропитание

3.1. Внедрение ошибок (fault injection)

Это активные атаки, когда хакер намеренно нарушает работу устройства, воздействуя на его питание или тактовую частоту. Самый распространенный метод — voltage glitching. Хакер в нужный момент кратковременно снижает напряжение. Процессор начинает ошибаться. В результате можно обойти проверку пароля или заставить устройство выдать секретные данные [3].

Еще один способ — электромагнитное воздействие. Специальным импульсом можно «ударить» по конкретному участку микросхемы и вызвать сбой [4].

3.2. Вывод техники из строя

Кроме кражи данных, электромагнитные импульсы могут просто сломать устройство. Мощный импульс создает в проводах разрушительное напряжение. Описаны случаи, когда из обычной фотовспышки и катушки делали портативный генератор, который выводил из строя домофоны и шлагбаумы с расстояния в несколько метров.

4. Как защититься от аппаратных атак

4.1. Экранирование и фильтрация

Чтобы сигналы не утекали наружу, устройство помещают в металлический корпус (экранируют). Это не дает излучению выйти за пределы устройства [5].

Для защиты от скачков напряжения используют фильтры питания: специальные конденсаторы сглаживают перепады. Также в процессорах есть датчики, которые при падении напряжения переводят устройство в безопасный режим.

4.2. Оптоволокно вместо проводов

Для передачи важных данных лучше использовать оптоволоконные кабели. В отличие от медных проводов, оптоволокно не создает электромагнитного поля. Поэтому перехватить сигнал по наводке невозможно. Оптоволокно также устойчиво к внешним помехам [6].

В квантовых системах связи оптоволокно используют для передачи ключей шифрования — такие системы теоретически невозможно взломать незаметно [7].

4.3. Аппаратные модули безопасности (HSM)

Самый надежный способ защитить вычисления — использовать специальные защищенные модули (HSM). Это отдельные устройства, которые выполняют все операции с ключами шифрования в изолированной среде. Они защищены от прослушивания: имеют экранирование, работают так, что их работа не зависит от обрабатываемых данных (чтобы нельзя было определить ключ по времени вычисления), и оснащены надежными генераторами случайных чисел [8].

Аппаратный хакинг показывает, что электроника — это поле битвы. Хакеры используют физические законы, чтобы красть данные или ломать устройства. Электромагнитные наводки, уязвимости питания и закладки в оборудовании — все это требует комплексной защиты.

Создавать безопасную технику нужно с самого начала: на этапе проектирования, производства и эксплуатации. Понимание физики работы электроники помогает не только строить устройства, но и предугадывать, как их могут взломать.

Список литературы:

1. Liu Ch. S., Wang F., Gould P., Yagemann C. SoK: A Beginner-Friendly Introduction to Fault Injection Attacks // arXiv. – 2025. – DOI: 10.48550/arXiv.2509.18341 (дата обращения: 20.02.2026).
2. Side Channel Attacks: When Strong Cryptography is not Enough // Utimaco. – 2025. – URL: https://utimaco.com/news/blog-posts/side-channel-attacks-when-strong-cryptography-not-enough (дата обращения: 21.02.2026).
3. Barenghi A., Breveglieri L., Koren I., Naccache D. Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures // Proceedings of the IEEE. – 2012. – Vol. 100, No. 11. – P. 3056–3076. – DOI: 10.1109/JPROC.2012.2188769 (дата обращения: 25.02.2026).
4. Trouchkine T., Bukasa S. K., Escouteloup M., Lashermes R., Fournier J. Electromagnetic Fault Injection against a System-on-Chip: Toward New Micro-Architectural Fault Models // arXiv. – 2019. – DOI: 10.48550/arXiv.1910.11566 (дата обращения: 01.03.2026).
5. Что такое электромагнитное экранирование? Подробное руководство по принципам, материалам и проектированию // VMT. – 2026. – URL: https://www.machining-custom.com/ru/blog/electromagnetic-shielding.html (дата обращения: 09.03.2026).
6. Оптические кабели: принцип работы и разница с медными // Secumarket. – 24.04.2025. – URL: https://secumarket.ru/news/opticheskie_kabeli__printsip_raboty (дата обращения: 10.03.2026).
7. Pirandola S., Andersen U. L., Banchi L. et al. Advances in Quantum Cryptography // Advances in Optics and Photonics. – 2020. – Vol. 12, No. 4. – P. 1012–1236. – DOI: 10.1364/AOP.361502 (дата обращения: 15.03.2026).
8. Mehta J. What is a Hardware Security Module? Comprehensive Guide // Certera. – 2024. – URL: https://certera.com/blog/what-is-hardware-security-module-hsm-comprehensive-guide/ (дата обращения: 20.03.2026).

References:

1. Liu Ch. S., Wang F., Gould P., Yagemann C. SoK: A Beginner-Friendly Introduction to Fault Injection Attacks // arXiv. – 2025. – DOI: 10.48550/arXiv.2509.18341 (access date: 02/20/2026).
2. Side Channel Attacks: When Strong Cryptography is not Enough // Utimaco. – 2025. – URL: https://utimaco.com/news/blog-posts/side-channel-attacks-when-strong-cryptography-not-enough (access date: 02.21.2026).
3. Barenghi A., Breveglieri L., Koren I., Naccache D. Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures // Proceedings of the IEEE. – 2012. – Vol. 100, No. 11. – P. 3056–3076. – DOI: 10.1109/JPROC.2012.2188769 (access date: 02/25/2026).
4. Trouchkine T., Bukasa S. K., Escouteloup M., Lashermes R., Fournier J. Electromagnetic Fault Injection against a System-on-Chip: Toward New Micro-Architectural Fault Models // arXiv. – 2019. – DOI: 10.48550/arXiv.1910.11566 (date of access: 01.03.2026).

5. What is Electromagnetic Shielding? A Detailed Guide to Principles, Materials, and Design // VMT. – 2026. – URL: https://www.machining-custom.com/ru/blog/electromagnetic-shielding.html (date of access: 09.03.2026).
6. Optical Cables: Operating Principle and Differences with Copper Cables // Secumarket. – 24.04.2025. – URL: https://secumarket.ru/news/opticheskie_kabeli__printsip_raboty (date of access: 10.03.2026).
7. Pirandola S., Andersen U. L., Banchi L. et al. Advances in Quantum Cryptography // Advances in Optics and Photonics. – 2020. – Vol. 12, No. 4. – P. 1012–1236. – DOI: 10.1364/AOP.361502 (accessed: March 15, 2026).
8. Mehta J. What is a Hardware Security Module? Comprehensive Guide // Certera. – 2024. – URL: https://certera.com/blog/what-is-hardware-security-module-hsm-comprehensive-guide/ (accessed: March 20, 2026).