

УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПРИ ФИЗИЧЕСКОМ ДОСТУПЕ: ВЕКТОРЫ АТАК И МЕТОДЫ ЗАЩИТЫ

И.Ю. Яковенко¹

¹ Поволжский государственный университет телекоммуникаций
и информатики, г. Самара
e-mail: ilya.a.yakovenko@gmail.com

Аннотация

Рассмотрены фундаментальные угрозы информационной безопасности, реализуемые при наличии физического доступа к оборудованию: атаки класса BadUSB, методы извлечения и изменения данных на накопителях, эксплуатация уязвимостей BIOS/UEFI и установка аппаратных имплантов. Представлен практический опыт реализации HID-атаки. Для каждого вектора предложены практические контрмеры.

Ключевые слова: физический доступ, BadUSB, HID-атака, BitLocker, Secure Boot, rootkit, аппаратные импланты, информационная безопасность.

Введение

Большинство моделей угроз в области информационной безопасности ориентированы на удалённые атаки: эксплуатацию уязвимостей сетевых сервисов, фишинг, компрометацию учётных данных. Однако физический доступ нарушителя к вычислительной технике открывает принципиально иной класс угроз, зачастую недооцениваемых при проектировании систем защиты. По данным ежегодного отчёта Verizon Data Breach Investigations Report, физические инциденты формируют устойчивую долю среди всех зафиксированных нарушений – особенно в категории внутренних угроз (insider threat) [1].

Целью настоящей работы является систематизация данных векторов атак, анализ технических мер противодействия и описание практического опыта автора. Основные векторы и соответствующие меры защиты представлены на рисунке 1.

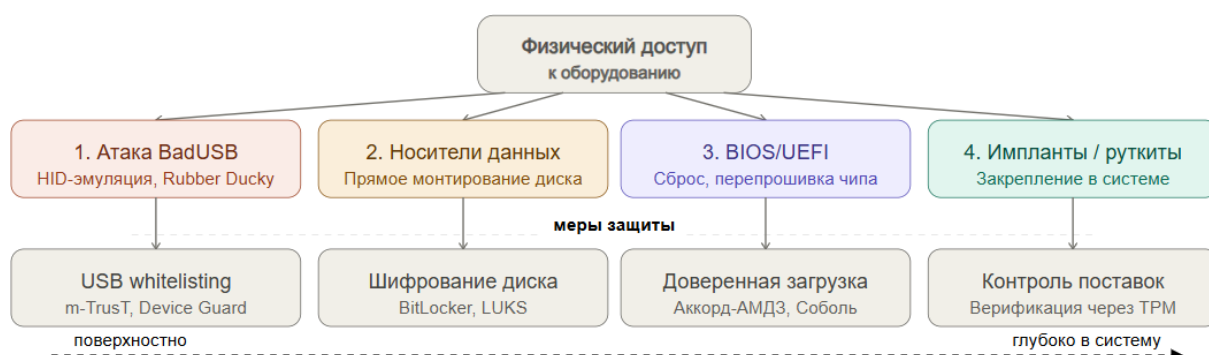


Рисунок 1 – Векторы атак и меры защиты информационных систем при физическом доступе к оборудованию

1. Атаки класса BadUSB

Атака BadUSB основана на перепрограммировании микроконтроллера USB-устройства таким образом, чтобы оно идентифицировалось операционной системой как устройство ввода (HID – Human Interface Device) [2]. Операционная система видит новое устройство как клавиатуру и начинает выполнять все поступающие с неё команды – автоматически и без каких-либо предупреждений. Эмуляция клавиатуры наиболее популярна, однако нарушитель может выбрать любой другой тип устройства: например, сетевую карту для перехвата трафика или загрузочный диск для запуска своей ОС.

В рамках подготовки к данной работе автором был приобретён модуль Digispark ATTINY85 стоимостью около 300 рублей на популярном маркетплейсе. Без специальной подготовки удалось реализовать эмуляцию HID-устройства и автоматический ввод 32-символьного пароля шифрования переносного накопителя по нажатию кнопки. Устройство внешне практически неотличимо от обычного USB-накопителя, что наглядно демонстрирует низкий порог входа для подобных атак даже без глубоких технических знаний.

Существуют меры защиты от подобных атак: групповые политики USB Device Guard (Windows) и usbguard (Linux) позволяют ввести белый список устройств по VID/PID. Для корпоративных сред применяется решение m-Trust (НПО «Эшелон»), реализующее аттестацию USB-устройств на уровне микроконтроллера. На объектах с повышенными требованиями безопасности, в частности в банковском секторе, практикуется физическое опломбирование неиспользуемых портов.

2. Атаки на носители данных

Все данные, интересующие нарушителя, хранятся на жёстком диске компьютера. Прямой доступ к ним преграждают пользовательский пароль входа, аутентификация в программах, права доступа. Но все эти механизмы просто не запустятся, если атакующий получает прямой доступ к диску.

Типичный сценарий: нарушитель, получив физический доступ к устройству на 10–15 минут, подключает внешний носитель с собственной ОС, загружается с него через boot-меню и монтирует внутренний диск. Файлы пользователя становятся доступны для чтения и копирования, а при аккуратных действиях вмешательство остаётся незамеченным после перезагрузки.

Самым действенным решением является полное шифрование жёсткого диска [3]: каждый байт зашифрован ключом, без знания которого данные нечитаемы, а любое изменение зашифрованного содержимого неизбежно повредит данные. Стойкость шифрования при длине ключа 16+ символов из расширенного набора делает перебор практически невозможным при современных вычислительных мощностях. В рамках данной работы автором применяется шифрование переносного SSD-накопителя средствами операционной системы: доступ к диску возможен только после ввода 32-символьного ключа, который автоматически вводится устройством на базе Digispark ATTINY85. Дополнительно рекомендуется установить пароль на BIOS/UEFI и запретить загрузку с внешних носителей.

3. Уязвимости прошивок BIOS/UEFI

Прошивка материнской платы – наиболее привилегированный компонент системы: код здесь выполняется раньше операционной системы и невидим для любых её защитных механизмов. Пользователи и производители защищают доступ к настройкам BIOS паролем, однако на практике эта защита ненадёжна. На многих системах после нескольких неудачных попыток ввода генерируется код, который преобразуется в мастер-ключ с помощью общедоступных онлайн-сервисов [4]. Альтернативный способ – извлечение CMOS-батарейки, хранящей настройки BIOS и пользовательский пароль.

Более серьёзная угроза – перепрошивка чипа BIOS или его замена на подготовленный, что позволяет встроить инструкцию, пережившую переустановку ОС и замену любых компонентов. Для защиты применяются пароль на BIOS Setup, физические пломбы на корпусе, а для организаций – аппаратные модули доверенной загрузки Аккорд-АМДЗ [5] или ПАК «Соболь» [6], берущие процесс загрузки под контроль до передачи управления прошивке.

4. Аппаратные импланты и программные руткиты

Это наиболее сложный для обнаружения вектор атаки: цель – незаметно закрепиться в системе на длительный срок. Программные руткиты уровня ядра перехватывают системные вызовы и работают с максимальными привилегиями. Операционная система воспринимает их код как собственный: процессы не отображаются в диспетчере задач, сетевые соединения скрыты, антивирус рапортует об отсутствии угроз.

В 2018 году компания ESET зафиксировала первый публично подтверждённый UEFI-руткит в реальных атаках – Lojах, применявшийся группой APT28: вредоносный код записывался в SPI Flash материнской платы и выживал после переустановки ОС и замены жёсткого диска [7]. Снизить риск помогают верификация целостности прошивок через TPM, применение сертифицированных модулей доверенной загрузки, а также контроль цепочки поставок оборудования.

Заключение

В работе рассмотрены четыре вектора атак при физическом доступе к оборудованию: эмуляция HID-устройств (BadUSB), извлечение данных с накопителей, эксплуатация уязвимостей BIOS/UEFI и установка аппаратных имплантов или руткитов. Практический эксперимент с модулем Digispark ATTINY85 подтвердил, что реализация HID-атаки доступна без специальной подготовки и при минимальных затратах.

Все рассмотренные угрозы представляют реальную опасность прежде всего для объектов с высокой ценностью данных: финансовых организаций, государственных учреждений, предприятий критической инфраструктуры. Для снижения рисков рекомендуется: 1) применять белые списки USB-устройств; 2) шифровать диск надёжным ключом; 3) устанавливать пароль на BIOS и запрещать загрузку с внешних носителей; 4) приобретать оборудование у доверенных поставщиков напрямую.

Дальнейшие исследования целесообразно направить на оценку эффективности отечественных средств защиты (m-TrusT, Аккорд-АМДЗ) в сравнении с зарубежными аналогами, а также на разработку методики обнаружения аппаратных имплантов.

Список использованных источников

1. Verizon. 2024 Data Breach Investigations Report. – URL: <https://www.verizon.com/business/resources/reports/dbir/> (дата обращения: 25.03.2026).
2. Nohl K., Lell J. BadUSB – On Accessories that Turn Evil // Black Hat USA 2014. – Las Vegas, 2014. – URL: https://assets.website-files.com/6098eeb4f4b0288367fbb639/62bc77c194c4e0fe8fc5e4b5_SRLabs-BadUSB-BlackHat-v1.pdf (дата обращения: 25.03.2026).
3. Изучаем и вскрываем BitLocker. Как устроена защита дисков Windows и как её взломать // Хакер. – URL: <https://xakep.ru/2017/02/23/bitlocker-hacking/> (дата обращения: 25.03.2026).
4. BIOS Password Recovery for Laptops: сайт. – URL: <https://bios-pw.org> (дата обращения: 27.03.2026).
5. ПАК СЗИ НСД «Аккорд-АМДЗ» // ОКБ САПР: официальный сайт. – URL: <https://www.okbsapr.ru/about/license/certificates/akkord-amdz/> (дата обращения: 27.03.2026).
6. ПАК «Соболь» // ООО «Код Безопасности»: официальный сайт. – URL: https://www.securitycode.ru/products/pak_sobol/ (дата обращения: 27.03.2026).
7. LoJax: First UEFI rootkit found in the wild // ESET Research: White Paper. – 2018. – URL: <https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf> (дата обращения: 28.03.2026).

VULNERABILITIES OF INFORMATION SYSTEMS UNDER PHYSICAL ACCESS: ATTACK VECTORS AND PROTECTION METHODS

I.Yu. Yakovenko¹

¹ *Volga State University of Telecommunications and Informatics*
e-mail: ilya.a.yakovenko@gmail.com

Abstract

The paper examines fundamental information security threats realized when physical access to equipment is available: BadUSB-class attacks, methods for extracting and modifying data on storage devices, exploitation of BIOS/UEFI vulnerabilities, and installation of hardware implants. Practical experience of HID-attack implementation is presented. Countermeasures are proposed for each attack vector.

Keywords: physical access, BadUSB, HID attack, BitLocker, Secure Boot, rootkit, hardware implants, information security.