



**USB-УГРОЗА:
JUICE JACKING**

ЧТО ТАКОЕ JUICE JACKING?

Это тип кибератаки, при котором злоумышленники используют возможности USB-порта зарядки для скрытой передачи данных или установки вредоносного ПО.

USB-разъём совмещает два канала: питание и данные. Если порт или кабель модифицирован, подключение к нему превращается в точку доступа для атаки.

Juice jacking опасен тем, что пользователь не видит никаких признаков взлома: телефон заряжается как обычно, экран не показывает предупреждений, а вредоносный код может устанавливаться в фоновом режиме.



МЕХАНИЗМ АТАКИ

Juice jacking опирается на базовую особенность USB-технологии: передача данных включена по умолчанию.

Этапы атаки:

1. В USB-станцию или кабель встраивается микроконтроллер для передачи команд или загрузки вредоносного кода.
2. Пользователь подключает смартфон к такой «зарядке» в общественном месте.
3. Устройство автоматически устанавливает драйверы или открывает файловую систему без подтверждения.
4. Злоумышленник получает доступ к данным (файлы, контакты, SMS) или устанавливает шпионское ПО.
5. Атака остаётся незаметной — пользователь видит только процесс зарядки.



ПОСЛЕДСТВИЯ JUICE JACKING

Кража данных: контакты, фото, документы, логины, пароли — всё это может быть скопировано через USB-канал.

Установка вредоносного ПО и удалённый контроль: шпионские программы, трояны, кейлоггеры или инструменты удалённого доступа могут быть установлены на устройство. Такое ПО обеспечивает злоумышленнику постоянный доступ, сохраняя контроль даже после отключения от заражённого порта.

Перехват SMS и уведомлений: это особенно опасно для банковских операций и двухфакторной аутентификации.

Клонирование устройства: некоторые вредоносные модули копируют структуру файловой системы, создавая цифровую копию смартфона.



ТОЧКИ РИСКА

Атакующие выбирают места, в которых люди заряжают устройства «на ходу» и не задумываются о безопасности: аэропорты, вокзалы, кафе, торговые центры и гостиницы. Отдельный риск — временные зарядные точки на конференциях и выставках, которые идеально подходят для скрытой модификации.

Также злоумышленники подбрасывают в людных местах **модифицированные кабели**, которые выглядят а**бсолютно** **нормальными**. находка воспринимается как случайная удача, что полностью отключает критику. Внутри такого «подарка» может скрываться чип, превращающий кабель в инструмент для мгновенного взлома в момент подключения.



МЕРЫ БЕЗОПАСНОСТИ

1. Личный кабель и зарядный блок — самый надёжный способ защиты. В крайнем случае обязательно используйте физический адаптер USB-data blocker.

2. Выбирайте обычные розетки, а не USB-порты. Розетка обеспечивает только питание, полностью исключая возможность передачи данных.

3. Включайте режим «Только зарядка». При подключении в появившемся системном уведомлении всегда выбирайте этот режим и не подтверждайте запросы на доверие устройству или доступ к данным.

4. Следите за поведением устройства. Любые необычные всплывающие окна или самопроизвольные действия — сигнал к немедленному отключению от зарядки.

