**Цена небезопасного проектирования**

**Введение**

В мире, где цифровые системы становятся всё сложнее, защита данных уже не сводится к написанию «правильного кода». Ошибки в архитектуре, бизнес-логике или взаимодействии пользователей могут быть такими же опасными, как баги в коде. Именно поэтому в обновлённой версии OWASP Top 10 за 2021 год появился пункт A04: Insecure Design — «Небезопасное проектирование» (OWASP Top 10, 2021). Это не просто техническая проблема, а системный просчёт, который может обойтись очень дорого.

**В чём суть?**

Небезопасное проектирование— это когда система изначально спроектирована с уязвимостями. Вот где он проявляется:

* **Отсутствие моделирования угроз.** Никто не задумался, как злоумышленники могут использовать систему.
* **Слепота к сценариям злоупотребления.** Бизнес-процессы не учитывают, как их могут обойти.
* **Недостаточная сегментация.** Сеть или данные не разделены на защищённые зоны.
* **Небезопасные настройки по умолчанию.** Система уязвима сразу «из коробки».

Самое неприятное — такие ошибки не исправить простым патчем. Нужно переделывать архитектуру, а это время, деньги и нервы.

**Реальные истории**

**1. Утечка данных Equifax (2017)**

В 2017 году компания Equifax потеряла данные 147 миллионов человек. Формально виной был устаревший компонент Apache Struts, но настоящая беда крылась в архитектуре:

* Веб-приложение напрямую лезло в базы данных без барьеров.
* Сеть не была разделена на сегменты.
* Процесс обновления софта был, мягко говоря, не на высоте.

Итог? Крупнейшая утечка персональных данных в истории США, миллиардные убытки и подмоченная репутация.  
*Источники:* [*Wikipedia — Equifax data breach*](https://en.wikipedia.org/wiki/2017_Equifax_data_breach)[*Mozilla Monitor*](https://www.mozilla.org/en-US/products/monitor/equifax-data-breach/)[*Majority Staff Report 115th Congress*](https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf)

**2. Ботнет Mirai (2016)**

Помните, как в 2016 году интернет «лёг» из-за DDoS-атак? Виновником был ботнет Mirai, который заразил сотни тысяч IoT-устройств — камер, роутеров и прочей техники. Почему? Производители ставили на устройства одинаковые логины и пароли по умолчанию, да ещё и открывали их в интернет. Это классический пример «небезопасного дизайна» — системы, уязвимой прямо с завода. Twitter, Netflix, Spotify и многие другие сервисы тогда серьёзно пострадали.  
*Источники:*

[*Wikipedia — Mirai (malware)*](https://en.wikipedia.org/wiki/Mirai_%28malware%29)[*Cloudflare — What is the Mirai Botnet?*](https://www.cloudflare.com/ru-ru/learning/ddos/glossary/mirai-botnet/)

**3. Zoom-бомбинг (2020)**

В начале пандемии Zoom стал спасением для удалённой работы, но тут же столкнулся с «Zoom-бомбингом». Злоумышленники врывались на чужие видеовстречи, срывая уроки и совещания. Почему так вышло?

* Идентификаторы встреч были предсказуемыми.
* Пароли по умолчанию не использовались.
* Контроль доступа был слабым.

Zoom пришлось срочно переделывать систему, но репутация уже пострадала.  
*Источники:* [*Wikipedia — Zoombombing*](https://en.wikipedia.org/wiki/Zoombombing)[*Tomsguide — Zoom security issues: What's gone wrong and what's been fixed*](https://www.tomsguide.com/news/zoom-security-privacy-woes)[*Сloud security alliance*](https://cloudsecurityalliance.org/blog/2022/03/13/an-analysis-of-the-2020-zoom-breach)

**Как этого избежать?**

Чтобы не повторять чужих ошибок, нужно думать о безопасности с самого начала:

* **Моделируйте угрозы.** Ещё на этапе проектирования представьте, как хакеры могут сломать вашу систему.
* **Делайте безопасно по умолчанию.** Настройки должны быть такими, чтобы пользователю не пришлось самому «закручивать гайки».
* **Разделяйте и ограничивайте.** Используйте сегментацию сети и принцип минимальных привилегий.
* **Стройте защиту вглубь.** Многоуровневая защита спасёт, если один слой пробьют.
* **Обновляйте вовремя.** Политика обновлений должна быть частью архитектуры.

**Заключение**

Небезопасное проектирование — это не просто строчка кода, которую можно исправить за пять минут. Это системные ошибки, которые приводят к утечкам данных, финансовым потерям и испорченной репутации. Истории Equifax, Mirai и Zoom — это напоминание: безопасность нужно закладывать с первого чертежа. Иначе цена ошибки может стать неподъёмной.