КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ИТОГИ

КОД ИБ ИТОГИ 2023

МОСКВА

07 ДЕКАБРЯ 2023

ПАЛЬМИРА БИЗНЕС КЛУБ

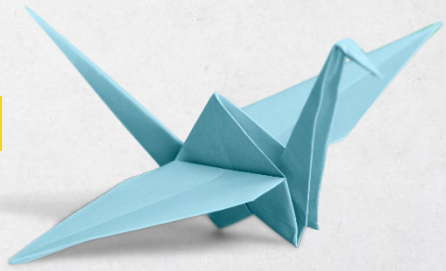
Рыночная статистика

- Фиксируется глобальный переход пользователей на мобильные платформы*. В IV квартале 2022 года ежедневно в Google Play загружалось более **1700** новых приложений.

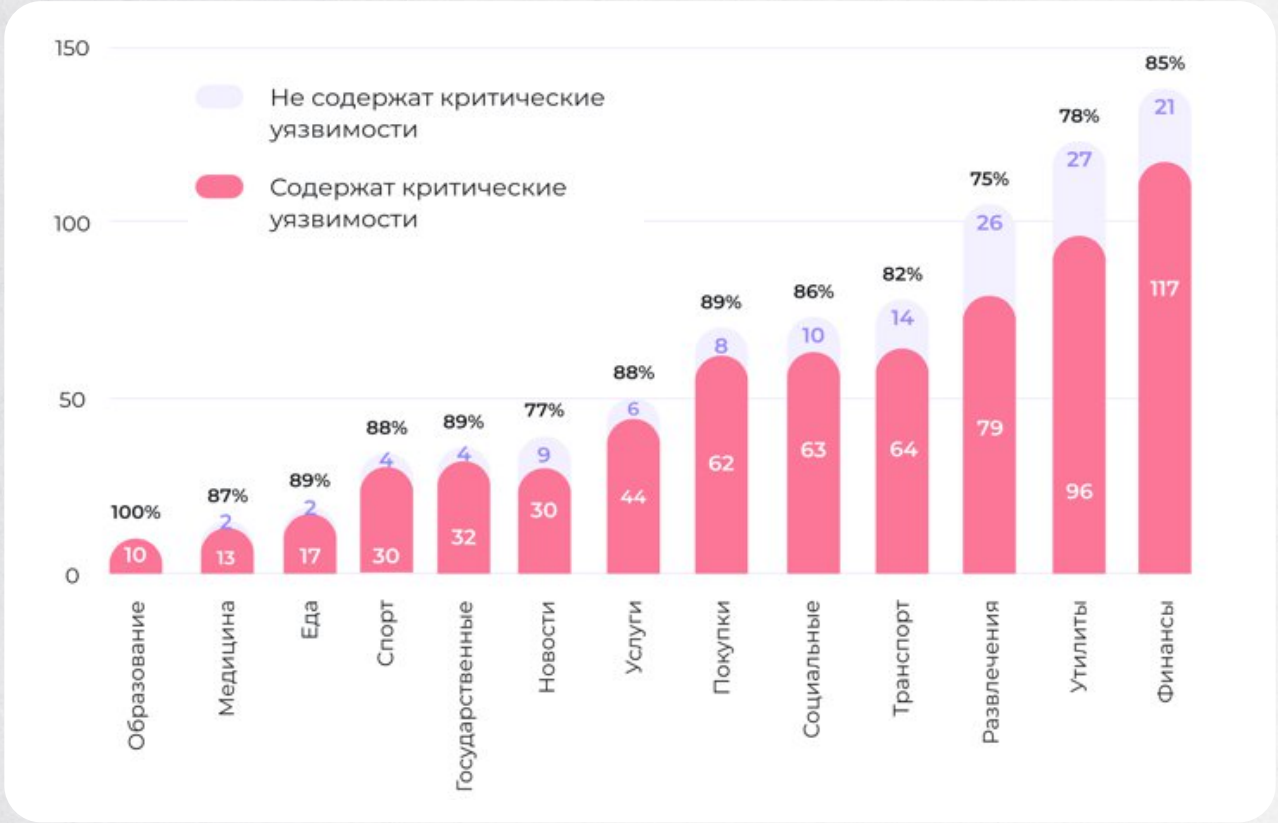
- В 2022 году россияне проводили в мобильных приложениях 4,5 часа в день**. По сравнению со вторым кварталом 2020 года, показатель вырос на 10%.

- По данным Тинькофф: уже в **2018** году пользователей мобильных версии банка стало превышать аналогичный показатель для Web-версии и этот разрыв продолжает расти

**По данным Marketsandmarkets.com*
***По данным Data.AI*

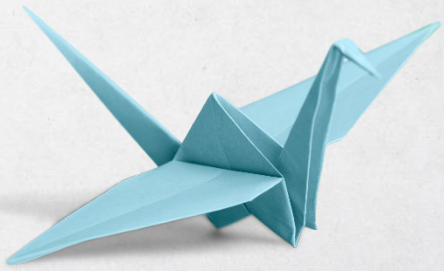


Безопасность мобильных приложений в 2022 году



83% мобильных приложений содержат уязвимости **высокого** и **критического** уровня*

** Согласно [исследованию Стингрей Технолоджиз](), опубликованному в конце 2022 года. С помощью платформы Стингрей было проанализировано **790** мобильных приложений из разных отраслей.*



Безопасность мобильных приложений в 2023 году

В новом исследовании проведен анализ 1817 приложений:

- Выявлено 22 критические уязвимости
- Выявлено 2383 уязвимости высокого уровня
- Как минимум **60%** приложений содержат уязвимости критического и высокого уровней

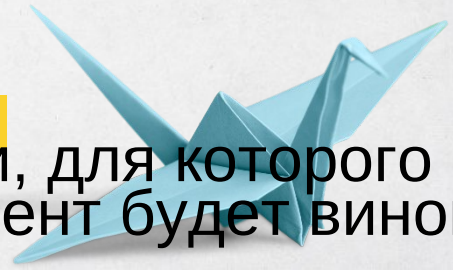
Почему все так?

Сложности с мобильными приложениями

- Мобильные приложения выполняются во враждебной среде на устройстве пользователя
- Нет возможности контролировать обновление приложения
- Исполняемый файл приложения находится в открытом доступе
- Есть возможность физического доступа к устройству, где работает приложение
- Большая фрагментация устройств
- Необходимость специально подготовленных устройств для проведения тестирования

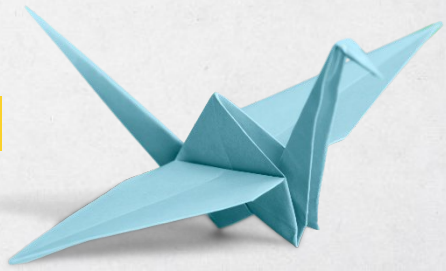
Распространенные заблуждения

- Мобильное приложение - это только один пользователь и его безопасность
- Приложение - это всего лишь витрина данных для серверной части системы
- Приложения и так проверяются на стороне Google и Apple перед публикацией
- Операционная система имеет встроенные механизмы, которые защищают данные приложений
- Атаки на мобильные приложения могут повлечь за собой не самый большой ущерб, который покроется рисками
- У мобильных приложений узкий вектор атаки, для которого часто необходим физический доступ, а значит, клиент будет виноват сам



ВЫВОДЫ

- Мобильные приложения заслуживают отдельного внимания со стороны безопасности
- Не стоит надеяться на мифические проверки магазинов приложений или считать, что это всего лишь отображение данных с серверной части. Это уже давно не так.
- Мобильные приложения сегодня - это неотъемлемая, а иногда и одна из главных частей всей системы



ВЫВОДЫ

Безопасность программ, которые мы используем каждый день, которые установлены у нас на телефоне, которые оперируют нашими данными, должна быть если не на первом плане, то хотя бы в тройке лидеров