

# РОССИЙСКИЕ МОБИЛЬНЫЕ СЕРВИСЫ

КАК ОСНОВА  
ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА  
РОССИИ

Дмитрий Алтухов

12 июля 2023 года

# Жизнь граждан России в смартфонах

- Более **100 миллионов** граждан РФ пользуются смартфонами\*
- В среднем россияне проводят в интернете **более 4 часов** в день\*\*
- На смартфоны приходится **90%** интернет-трафика\*

\* <https://datareportal.com/reports/digital-2023-russian-federation>

\*\* MEDIASCOPE CROSS WEB, ВСЯ РОССИЯ, АПРЕЛЬ 2023

# Кому принадлежит жизнь граждан РФ в смартфоне?

## Аппаратное обеспечение

### «Мозг»

(процессор и ключевые компоненты) – США или Тайвань



«Железо» (комплектующие) – Тайвань, Южная Корея, КНР



«Сборка» (производство устройств) – КНР, Индия, Вьетнам, Южная Корея



## Программное обеспечение

Мобильные операционные системы – США, КНР



Мобильные сервисы – США, КНР



Встроенные магазины приложений – США, КНР, Южная Корея



**Национальная безопасность? Технологический суверенитет?**

# Основные угрозы в мобильных технологиях

## Сбор данных и слежка за пользователями со стороны владельцев ОС и сервисов

- хранение персональных данных за пределами РФ в **недружественных странах**
- полный набор телеметрии (IP адрес, геолокация, сетевая активность)
- профилирование и выбор приоритетных целей для возможных атак

## Наличие технических возможностей у владельцев ОС и сервисов

- **нарушить работу приложений:** отключение сервисов, удаление приложений из магазинов, дистанционная блокировка/удаление приложений на устройствах)
- **дистанционно отключить устройства:** сброс с удалением всех данных, вывод устройств из строя (документированные функции + НДВ)
- провести **массовую рассылку** сообщений (документированные функции + НДВ)

## Отсутствие суверенитета

- мобильные технологии являются «фундаментом» для целого ряда сквозных технологий
- более 90% мобильных устройств и ОС полностью контролируется иностранными государствами
- полная зависимость от иностранных технологий
- импортозамещение смартфонов и мобильных ОС почти не ведётся



# Мобильное устройство – платформа сбора данных

- Второй экран, а часто и замена компьютера
- Устройство всегда с собой, постоянно собирает и передаёт данные в недружественные страны\*
- Делает это и на объектах КИИ



\* Leith, D.J. (2021). Mobile Handset Privacy: Measuring the Data iOS and Android Send to Apple and Google. *Security and Privacy in Communication Networks*. H. Liu, P. Patras, and D. J. Leith, "Android Mobile OS Snooping By Samsung, Xiaomi, Huawei and Realme Handsets," in SCSS Tech Report, Oct 2021, 2021.

# Современные мобильные экосистемы

Облачные сервисы, приложения и API

Операционная система

Драйверы и ядро ОС

# Архитектура верхнего уровня

В мобильной экосистеме «бутылочное горлышко» конкуренции – не ОС, а облачные сервисы



# Импортозамещение и КИИ

## • Desktop

- Организации: нормативы по переходу на российские настольные и серверные ОС, оборудования определены и реализуются для госсектора и крупного бизнеса, в образовании
- Граждане: продолжают использовать американскую ОС Windows



## • Mobile

- Организации:
  - Нормативы по переходу на российские мобильные ОС и оборудование **не** определены, продолжают использовать устройства с американскими ОС Android и iOS
  - Переход на российские решения не затрагивает мобильные – типичный ответ: *«это устройства работников и не участвуют в основных процессах»*
  - В том числе, на значимых объектах КИИ
- Граждане: продолжают использовать устройства с американскими ОС Android и iOS



# Регулирование и КИИ

- Формального запрета использовать иностранные мобильные ОС в госсекторе и корпоративном сегменте в России на данный момент нет.
- Ограничения по использованию иностранного ПО с 2025 года сегодня касаются только значимых объектов КИИ и не касаются мобильных устройств.
- Отсутствуют нормативные документы, определяющие требования и профили безопасности корпоративных мобильных платформ, регламенты использования мобильных платформ.

# Текущая ситуация в разработке и производстве современных мобильных устройств





# Технологический суверенитет

2023-2025

2026-2028

2029-2030

## Снижение рисков для РФ

- защита граждан от угроз блокировки устройств, приложений и сервисов со стороны недружественных стран
- сохранение возможности использования Android-приложений в переходный период
- разработка российских мобильных сервисов (PMC) для замены иностранных
- миграция ключевых B2C приложений на российскую мобильную ОС
- ускорение перехода на российскую мобильную ОС в B2G и B2B

## Технологический суверенитет РФ

- PMC на большинстве смартфонов в B2C
- только российская мобильная ОС с PMC в B2G и B2B с госучастием
- выход российской мобильной ОС с PMC на B2C рынок
- заметную долю рынка занимают смартфоны российских производителей
- реализуется экспортный потенциал PMC и мобильной ОС в дружественных странах

## Технологическое лидерство РФ

- Россия входит в Топ-5 стран по уровню развития технологий мобильности
- существенную долю рынка занимают смартфоны российских производителей с российской мобильной ОС с PMC
- PMC и мобильная ОС успешно конкурируют на международных рынках

## Реально ли выйти из мобильной «колеи»?

- Ключевой фактор в мобильных экосистемах – **облачные сервисы и API**, обеспечивающие сетевую функциональность устройств. Магазин и push – совершенно недостаточно!
- **GMS и HMS – не вариант для России. Наш возможный путь – национальный стандарт экосистемы, российские мобильные сервисы.**
- Необходимо через **долгосрочное** сотрудничество (а не конкуренция) **всех** ключевых участников российской экосистемы.
- Размер рынка России не оставляет места для конкуренции, более того, необходим экспорт экосистемы в дружественные страны.



# РМС: определение и основные особенности

**Кроссплатформенный набор приложений, сервисов и API, работающий на устройствах как с Android/AOSP, так и с российскими ОС («Аврора», «Астра»).**

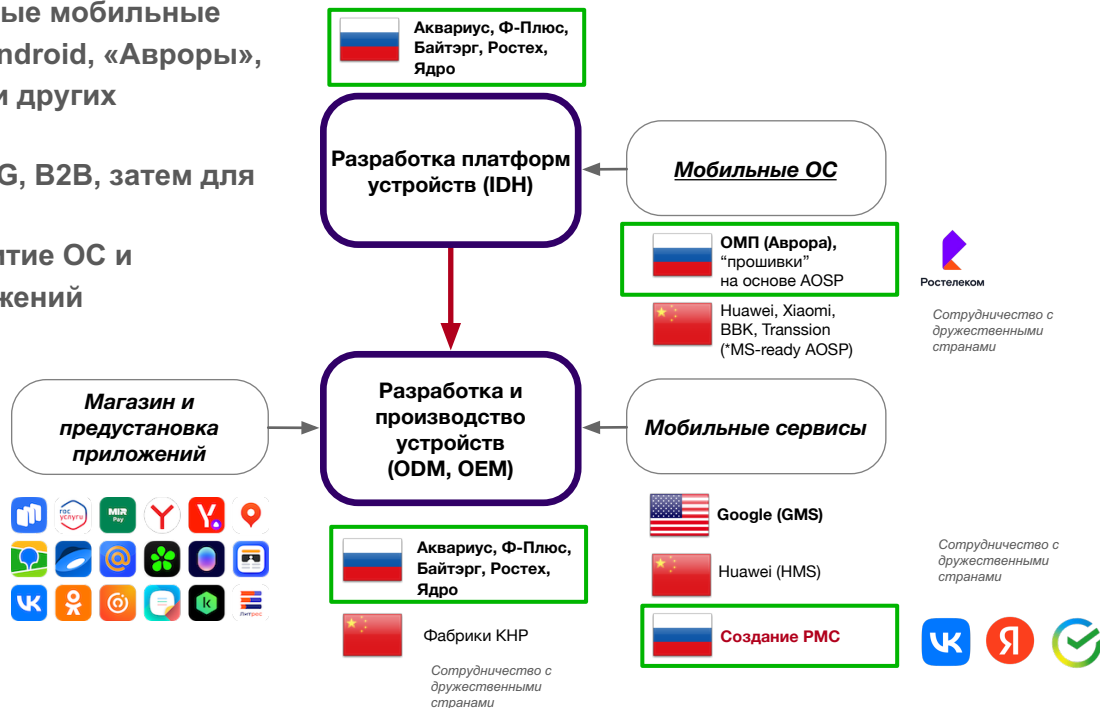
**Серверная (облачная) составляющая размещена в РФ.**

**Обеспечивают функциональность, аналогичную GMS и HMS.**

- **РМС должны формироваться как единая библиотека, устанавливаемая на все мобильные устройства**
- Ключевые уникальные сервисы только у оператора РМС :
  - критические облачные сервисы,
  - Push-сообщения,
  - магазин приложений,
  - проверка подлинности,
  - криптография
- Рыночные сервисы открыты для участников рынка (карты, облачные хранилища, банковские приложения и т. д.)
- Предустановка на российские и официально импортируемые устройства
- В первые 2–3 года установка РМС пользователями на существующие устройства и ввезённые через параллельный импорт
- Цель – к 2030 году большая часть «белого» рынка РФ на устройствах с РМС:
  - российская криптография только на устройствах без иностранных сервисов
  - госуслуги и платёжные приложения только на устройствах с российской криптографией

# Три основных вектора на пути к суверенитету

1. Российские кроссплатформенные мобильные сервисы (PMC) и RuStore для Android, «Авроры», мобильной версии Astra Linux и других российских ОС
2. Российские смартфоны для B2G, B2B, затем для B2C
3. Мобильная ОС «Аврора»: развитие ОС и наполнение экосистемы приложений



# Смартфон через 5-7 лет

## Аппаратное обеспечение

### «Мозг»

(процессор и ключевые компоненты) –  
КНР. Тайвань и США.



«Железо» (комплектующие) –  
КНР, РФ, Тайвань.



«Сборка» (производство устройств) –  
КНР, РФ. Индия, Вьетнам



## Программное обеспечение

Мобильные **операционные системы** –  
РФ. Частично КНР и США.



Мобильные **сервисы** –  
РФ. Частично КНР и США.



Встроенные **магазины приложений** –  
РФ. Частично КНР и США.





# РМС – основа технологического суверенитета

- Создание РМС обеспечит независимость в мобильности от облачных сервисов американских корпораций, фундамент технологического суверенитета России в мобильных технологиях.
- Только комплексный подход, системно поддерживаемый государством, восстановление отрасли микроэлектроники и строительство заводов, обеспечивающих массовое производство современных микросхем и SoC смогут обеспечить приближение к полноценному суверенитету.
- Дорога на десятилетия, инвестиции, сопоставимые с ежегодным бюджетом РФ, но это путь, при котором РФ действительно сможет стать одним из значимых центров будущего многополярного мира.

# Спасибо за внимание!

Лекция в Финансовом университете «Мобильные экосистемы и технологический суверенитет»

