Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

18 настроек Android: защита трафика гендиректора юрфирмы

Наша методика: ADB-аудит, Private DNS, always-on WireGuard, work-профиль и контур на MikroTik

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Смартфон руководителя юрфирмы — это переписка по сделкам, сканы документов и доступ к банкам. Штатный Android шлёт фоновую телеметрию десяткам доменов вендора, Google и рекламных сетей: DNS-запросы видны оператору, captive-portal-пробы и облачные синхронизации уходят в чужие дата-центры. Без харденинга утечка метаданных и адресная разведка конкурентов — вопрос времени.

Почему это важно бизнесу

- Метаданные переписки и геолокация руководителя — готовый материал для конкурентной разведки по сделкам
- Фоновая телеметрия в сотни МБ/сутки — это контакты, заметки и календарь в чужих облаках вне контроля компании
- Компрометация одного смартфона обесценивает NDA и адвокатскую тайну — ущерб несравним со стоимостью аудита
- Разовая настройка без сопровождения деградирует за 6-9 месяцев: обновления возвращают отключённые службы

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

DoT :853

Private DNS на наш AdGuard-резолвер; задаём строгий hostname, не Automatic

Android 9+, наш резолвер

v30.7

Magisk+Zygisk: DenyList отключает Magisk в процессах 11 банков и гос-приложений; работу каждог…

релиз Magisk, 02.2026

0.0.0.0/0

AllowedIPs WireGuard (плюс ::/0) + lockdown «Блокировать без VPN» — мимо туннеля трафик не ухо…

по докам Android/WireGuard

9+9

9 служб гасим через pm disable-user --user 0, 9 защит добавляем — наш чек-лист из 18 пунктов

наш стандарт

90 дней

Интервал контрольного визита: обновления Samsung/Google возвращают отключённые пакеты

наш стандарт

≤25 МБ

Порог фонового трафика в сутки после работ; выше — повод для внепланового разбора логов

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Настольный аудит по ADB на изолированном стенде

Что настраиваем

Смартфон руководителя (Samsung, One UI); стенд — ноутбук с изолированной Wi-Fi-точкой и записью трафика tcpdump

Как мы это делаем

1. adb bugreport + pm list packages -i/-s/-d: полная карта пакетов с источником установки; отдельно dumpsys usagestats по фоновой активности каждого приложения
2. adb shell ss -tunap и /proc/net/{tcp,udp}: активные соединения, сверяем с пакетами — ищем периодические коннекты облачных синхронизаций каждые 3-4 минуты
3. Проверка CA-хранилищ: /data/misc/user/0/cacerts-added на посторонние пользовательские сертификаты, системное /system/etc/security/cacerts — сверка с эталоном
4. Матрица разрешений: приложения с фоновой геолокацией и чтением SMS, не запускавшиеся 30+ дней, — первые кандидаты на удаление

РЕЗУЛЬТАТ

Полная карта аппарата за 90 минут без касания чужих сетей: кто и как часто ходит в сеть, у каких пакетов избыточные разрешения, нет ли внедрённых сертификатов. Отключаем не «по списку из интернета», а по фактической активности конкретного телефона.

КЛЮЧЕВОЙ НЮАНС

Аудит — до любых изменений и только через изолированную точку: bugreport фиксирует базовую линию трафика, с которой потом сравниваем контрольный замер на приёмке.

РЕАЛИЗАЦИЯ 2 ИЗ 3

18 пунктов на аппарате: службы, DNS, root-контур

Что настраиваем

Сам смартфон: системные службы вендора и Google, DNS, магазины приложений, work-профиль

Как мы это делаем

1. pm disable-user --user 0 для телеметрии вендора (Knox customization, Bixby, scloud, gametuner) и периферии Google (feedback, partnersetup, captiveportallogin)
2. settings put global captive_portal_mode 0 (MODE_IGNORE) — убираем фоновые connectivity-probe; гасим фоновое Wi-Fi/BT-сканирование в настройках геолокации
3. Private DNS строгим hostname нашего AdGuard-резолвера (DoT, 853/TCP); поле в Android одно — запасной hostname dns.quad9.net фиксируем в паспорте настройки; отзываем…
4. Magisk v30.7 + Zygisk, DenyList на банки/Госуслуги/ФНС — прогон каждого приложения на приёмке; AFWall+ в режиме default-deny; F-Droid и Aurora Store в анонимном реж…
5. Work-профиль Android Enterprise (Shelter): мессенджеры и рабочие приложения переезжают в отдельный шифрованный профиль с собственным keystore

РЕЗУЛЬТАТ

Фоновый трафик падает с сотен МБ до ≤25 МБ/сутки (остаются push FCM и обновления), телеметрия и рекламные сети отрезаны, при этом звонки, биометрия, банковские и государственные приложения работают штатно.

КЛЮЧЕВОЙ НЮАНС

Ядро Google Play Services не трогаем — это транспорт FCM-push; режем только периферию. Разблокировка загрузчика необратимо жжёт Knox e-fuse — этот шаг согласуем письменно.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Сетевой контур: WireGuard, VLAN и контроль на MikroTik

Что настраиваем

Офисный MikroTik CCR-класса на RouterOS 7.x + наш VPN-узел с AdGuard Home в дата-центре

Как мы это делаем

1. Always-on WireGuard с lockdown («Блокировать соединения без VPN»); исключения — только антифрод-чувствительные банки через lockdown-allowlist setAlwaysOnVpnPackage…
2. Отдельная VLAN устройств руководства: /interface vlan + mangle mark-routing в туннель — выход только через VPN, полная изоляция от LAN с 1С и файловыми шарами
3. DNS-фильтрация на AdGuard Home v0.107: блок-листы рекламы, телеметрии и C2-доменов; блокируем на этапе резолва, до TLS-handshake — pinning приложений не мешает
4. Remote syslog всех соединений устройства на отдельный сервер: алерты на аномальные направления и ночную активность
5. Приёмка через mitmproxy 12.x в transparent mode: прогон банков и гос-сервисов, контроль нулевых обращений к рекламным и облачным доменам вендора

РЕЗУЛЬТАТ

Даже если обновление вернёт отключённую службу, её трафик упрётся в DNS-фильтр и файрвол контура, а попытка станет видна в syslog в течение часа. Защита перестаёт зависеть от одного слоя на самом телефоне.

КЛЮЧЕВОЙ НЮАНС

L2-правила по MAC работают только если для доверенной SSID зафиксирован «MAC устройства»: Android 10+ по умолчанию рандомизирует MAC на каждую сеть.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **pm uninstall вместо disable-user**
  uninstall --user 0 ломает откат и OTA-сценарии; disable-user обратим одной командой и легче переживает обновления прошивки

- ✕ **Private DNS в режиме «Автоматически»**
  Automatic откатывается на резолвер оператора. Фиксируем hostname: падение нашего DoT остановит сеть заметно — это безопаснее тихой утечки

- ✕ **MITM-проверка через user CA**
  С Android 7 приложения не доверяют user-хранилищу сертификатов — «чистый» результат будет ложным. Для приёмки нужен CA в системном хранилище

- ✕ **MAC-рандомизация против L2-фильтров**
  Случайный MAC на SSID обнуляет VLAN- и bridge-правила. Для доверенной сети выбираем «MAC устройства», для чужих оставляем рандомизацию

- ✕ **Обновления возвращают службы**
  Samsung/Google реактивируют пакеты при апдейтах. Закладываем визит раз в 90 дней со сверкой pm list packages -d против эталонного списка

- ✕ **Разблокировка загрузчика = Knox 0x1**
  E-fuse необратим: отпадают Samsung Pay и Secure Folder. Согласуем письменно, оплату переводим на NFC-кошельки банковских приложений

- ✕ **Lockdown-VPN без исключений**
  Антифрод банков чувствителен к выходному IP туннеля — вносим их в lockdown-allowlist (setAlwaysOnVpnPackage, API 29+), иначе ложные блокировки платеж…

- ✕ **Отключение Play Services «за компанию»**
  gms — транспорт push-уведомлений FCM. Гасим только сопутствующие пакеты (feedback, partnersetup), ядро не трогаем

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Private DNS (DoT) строгим hostname на корпоративный AdGuard-резолвер
- Ревизия через ADB: disable-user телеметрии, отзыв фоновой геолокации и чтения SMS
- Отключение captive-portal-проб (captive_portal_mode 0) и фонового Wi-Fi/BT-сканирова…

НОРМАЛЬНО

- Work-профиль Android Enterprise: рабочие приложения в отдельном шифрованном профиле
- Always-on WireGuard с lockdown «Блокировать соединения без VPN»
- Отдельная VLAN устройств руководства с выходом только через VPN-туннель

ХОРОШО

- Root-контур: Magisk DenyList, AFWall+ default-deny, F-Droid/Aurora вместо входа в Go…
- Remote syslog соединений смартфона с алертами на аномальные направления
- Приёмка mitmproxy + контрольный пересмотр настроек каждые 90 дней

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Private DNS задан строгим hostname корпоративного резолвера, а не режимом «Автоматически»?
- [ ] Always-on VPN включён вместе с lockdown — трафик блокируется, если туннель упал?
- [ ] Рабочие мессенджеры и почта живут в work-профиле Android Enterprise, а не в личном?
- [ ] Список отключённых служб сверяется после каждого обновления прошивки (pm list packages -d)?
- [ ] В пользовательском хранилище CA нет посторонних сертификатов (cacerts-added пуст)?
- [ ] Фоновое Wi-Fi/Bluetooth-сканирование и captive-portal-детект отключены?
- [ ] MAC-адрес зафиксирован для доверенной SSID, а в чужих сетях рандомизируется?
- [ ] DenyList закрывает все банковские и гос-приложения, каждое проверено запуском на приёмке?
- [ ] Соединения смартфона пишутся на syslog, и назначен ответственный за разбор аномалий?
- [ ] Фоновый трафик после работ замерен, укладывается в ≤25 МБ/сутки и зафиксирован в отчёте?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Настольный ADB-аудит смартфона руководителя с отчётом: пакеты, соединения, сертификаты, разрешения
- Настройка 18 пунктов защиты: службы, Private DNS, work-профиль, always-on WireGuard, root-контур по согласованию
- Сетевой контур офиса: VLAN руководства на MikroTik, AdGuard Home, syslog-мониторинг с алертами
- Приёмочная проверка mitmproxy и квартальное сопровождение — контроль возврата служб после обновлений

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Android Enterprise: Always-on VPN и lockdown (setAlwaysOnVpnPackage) (developer.android.com — 2026)

02 Android Enterprise Help: work-профиль и настройка VPN (support.google.com — 2026)

03 Magisk Documentation: Zygisk, DenyList, changelog (topjohnwu.github.io — v30.7)

04 AdGuard Home: DNS-фильтрация, блок-листы, DoT (github.com — v0.107.78)

05 RouterOS: VLAN, Firewall/Mangle, WireGuard (help.mikrotik.com — 7.x)

06 mitmproxy: transparent proxy mode (docs.mitmproxy.org — 12.x)

07 Наш чек-лист «18 пунктов Android-hardening» (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.