Выявление слежки в 30 популярных российских приложениях

Метод: статический анализ APK (декомпиляция, поиск по 68 контрольным точкам слежки в 12 категориях)
Объём выборки: 30 приложений из RuStore и Google Play

Оглавление

Ключевые выводы

- 22 из 30 приложений детектируют VPN, из них 18 подтверждённо отправляют VPN-статус на сервер
- 29 из 30 приложений проверяют наличие root-доступа (все кроме Яндекс Go)
- 24 из 30 запрашивают доступ к микрофону
- 28 из 30 запрашивают доступ к камере
- 24 из 30 отправляют список установленных приложений на свои серверы
- 11 из 30 приложений получают рейтинг RED (максимальная слежка)
- 49 из 68 проверок слежки работают без участия пользователя — сразу после установки

База данных анализа доступна по ссылке.

1. Какие приложения следят за VPN? (22 из 30)

Что это значит

Когда приложение детектирует VPN, оно фиксирует то, что пользователь скрывает свой реальный IP-адрес. Эта информация может передаваться на серверы компании, а оттуда — по запросу правоохранительных органов.

Методы детекции VPN, используемые приложениями

Метод	Что делает	Сколько приложений
`TRANSPORT_VPN`	Прямой API-запрос к Android: «включён ли VPN?»	16
Сетевые интерфейсы `tun0`	Перечисление сетевых адаптеров — VPN создаёт виртуальный `tun0`	14
Чтение `/proc/net/tcp`	Низкоуровневое чтение сетевых таблиц ядра Linux для детекта VPN-портов	4
Проверка proxy-настроек	Чтение системных свойств `http.proxyHost`	9
Отправка VPN-статуса на сервер	VPN-флаг передаётся в телеметрию	19
Детект Tor	Поиск пакетов `org.torproject.torbrowser`	1

Рейтинг приложений по глубине VPN-слежки

Приложение	Методов детекта	Что именно делает
Яндекс Браузер	**4**	TRANSPORT_VPN + /proc/net/tcp + tun0 + **детект Tor** + **→сервер**
Яндекс Карты	**4**	TRANSPORT_VPN + /proc/net/tcp + tun0 + proxy
ВКонтакте	3	TRANSPORT_VPN + tun0 + proxy + **→сервер**
Мой МТС	3	TRANSPORT_VPN + tun0 + proxy + **→сервер**
Сбербанк Онлайн	3	TRANSPORT_VPN + tun0 + proxy + **→сервер** (`setVpn()` в clickstream)
Т-Банк	3	/proc/net/tcp + tun0 + **→сервер** (`isVpnConnected` в fingerprint)
VK Видео	2	TRANSPORT_VPN + proxy + **→сервер**
Wildberries	2	tun0 + proxy
Кинопоиск	2	TRANSPORT_VPN + tun0 + **→сервер**
Ozon	2	TRANSPORT_VPN + proxy + **→сервер**
Самокат	2	TRANSPORT_VPN + tun0 + **→сервер**
RuStore	2	TRANSPORT_VPN + proxy + **→сервер**
ВТБ Онлайн	2	TRANSPORT_VPN + tun0 + **→сервер** (`is_vpn_on` в NetworkSettingsDto)
Yandex Music	2	/proc/net/tcp + tun0
VK Music	2	TRANSPORT_VPN + tun0 + →сервер (is_vpn в каждом stat-событии)
Avito	1	TRANSPORT_VPN + **→сервер**

Приложение	Методов детекта	Что именно делает
Альфа-Банк	1	proxy + →**сервер**
2ГИС	1	TRANSPORT_VPN + →**сервер**
MegaMarket	1	tun0 + →**сервер**
Одноклассники	1	TRANSPORT_VPN + →**сервер**
MAX	1	TRANSPORT_VPN + →**сервер**
Rutube	1	tun0 + →**сервер** (`VpnStatusResponse` API)

Приложения, которые НЕ детектируют VPN (8 из 30)

Итого: 8 из 30 приложения не детектируют VPN.
Яндекс Маркет, Яндекс Еда, Почта Mail.ru, МегаФон, Mir Pay, Госуслуги, Яндекс Go, Дзен.

Вывод: Яндекс Браузер — единственное приложение, которое ищет Tor на устройстве. Яндекс Браузер и Яндекс Карты используют максимальное число методов VPN-детекции (4 из 6). **19 из 22** приложений с VPN-детектом подтверждённо отправляют VPN-статус на свои серверы — в том числе Т-Банк (`@SerialName("isVpnConnected")`), Сбербанк (clickstream-аналитика), ВТБ (`@SerializedName("is_vpn_on")`), Яндекс Браузер (`vpn_enabled` в телеметрии) и Rutube (`VpnStatusResponse` API). MAX **обфусцирует** имена сетевых интерфейсов (tun/ppp/tap/pptp0 закодированы байтовыми массивами), что свидетельствует о намеренном сокрытии VPN-детекции от исследователей.

2. Самые жёсткие приложения по совокупности слежки

Рейтинг по числу сработавших проверок из 68:

#	Приложение	Рейтинг	Score	VPN	VPN → Сервер	Главная находка
1	**Т-Банк** Банк	RED	**65/68**	3	да	Ищет Frida через /proc/net/tcp:27042, `isVpnConnected` в fingerprint
2	**MegaMarket** Маркетплейс	RED	**65/68**	1	да	GPS каждые 2 сек, com.group_ib.sdk, контакты+SMS+журнал звонков
3	**ВКонтакте** Соцсеть	RED	**64/68**	3	да	IMEI/IMSI через reflection (обход Android 10), синхронизация контактов
4	**Одноклассники** Соцсеть	ORANGE	**64/68**	1	да	DeviceAdmin спрятан в модуле «эмодзи»
5	**Сбербанк Онлайн** Банк	RED	**64/68**	3	да	Касания: X/Y/давление/размер, VPN в clickstream
6	**Яндекс Браузер** Браузер	RED	**63/68**	4	да	Tor-детект + `vpn_enabled` в телеметрии + WhoCalls
7	**Яндекс Карты** Навигация	ORANGE	**60/68**	4	?	VPN-детект в собственном коде (не SDK)
8	**ВТБ Онлайн** Банк	RED	**59/68**	2	да	`is_vpn_on` в NetworkSettingsDto → сервер диагностики

#	Приложение	Рейтинг	Score	VPN	VPN → Сервер	Главная находка
9	**Rutube** Видео	ORANGE	**57/68**	1	да	Fraud-SDK шлёт список приложений + `VpnStatusResponse` API
10	**Альфа-Банк** Банк	ORANGE	**56/68**	1	да	Kaspersky SDK читает ВСЕ уведомления
11	**Мой МТС** Телеком	RED	**56/68**	3	да	ACCESS_SUPERUSER в манифесте, MTS GEO SDK
12	**Ozon** Маркетплейс	RED	**56/68**	2	да	247 банков + контакты в JSON → WebView
13	**Wildberries** Маркетплейс	RED	**55/68**	2	?	Фоновый перехват буфера обмена + полный журнал звонков
14	Самокат Доставка	RED	54/68	2	да	Список VPN-приложений — в доставке еды
15	Кинопоиск Стриминг	ORANGE	53/68	2	да	vpn_enabled + GPS отправляются на сервер
16	RuStore App Store	RED	53/68	2	да	Магазин приложений следит за VPN
17	Yandex Music Музыка	ORANGE	53/68	2	?	Frida-детект в музыкальном плеере
18	VK Music Музыка	ORANGE	52/68	2	да	tun0 + TRANSPORT_VPN, is_vpn в каждом событии, russian_trusted_root_ca
19	VK Видео Видео	ORANGE	51/68	2	да	3 SDK ищут VPN, контакты → vk.com
20	2ГИС Навигация	ORANGE	51/68	1	да	80+ банков + контакты через JNI → native код
21	Госуслуги Госуслуги	ORANGE	51/68	—	—	Тайминг нажатий в гос. приложении

#	Приложение	Рейтинг	Score	VPN	VPN → Сервер	Главная находка
22	Дзен Медиа	ORANGE	49/68	—	—	GPS каждые 2 сек для ленты новостей
23	Яндекс Еда Доставка	ORANGE	48/68	—	—	Тройная геолокация: GPS + вышки + WiFi
24	Avito Объявления	ORANGE	46/68	1	да	~200 чужих пакетов в queries манифеста
25	MAX (TamTam) Мессенджер	ORANGE	46/68	1	да	VPN-имена обфусцированы байт-массивами
26	МегаФон Телеком	ORANGE	41/68	—	—	Контакты выгружаются каждые 24 часа
27	Яндекс Маркет Маркетплейс	ORANGE	40/68	—	—	is_rooted в каждом HTTP-запросе
28	Почта Mail.ru Почта	ORANGE	40/68	—	—	Сервер решает, какие приложения искать
29	Яндекс Go Такси	ORANGE	39/68	—	—	Нет VPN/root-детекта — единственный из 30
30	Mir Pay Платежи	ORANGE	35/68	—	—	99% кода скрыто за libprotector.so

Кто лидирует по категориям

Банковские приложения — самая агрессивная группа. Т-Банк (65), Сбербанк (64) и ВТБ (59) входят в топ-10. Все три отправляют VPN-статус на серверы, используют расширенный fingerprinting устройства, детект рута и инструментов анализа.

Экосистема VK — ВКонтакте (64), Одноклассники (64), VK Видео (51). Объединяет VK Push SDK, ok.tracer, MyTracker. ВКонтакте и Одноклассники имеют одну из самых масштабных фоновых инфраструктур (67 и 77 сервисов соответственно).

Экосистема Яндекса — Браузер (63), Карты (60), Кинопоиск (53), Музыка (53). Объединяет AppMetrica, AppsFlyer. Яндекс Браузер — единственное приложение с детектом Tor и передаёт `vpn_enabled` в аналитику.

Маркетплейсы — MegaMarket (65), Ozon (56), Wildberries (55). MegaMarket (принадлежит Сберу) делит первое место с Т-Банк, использует com.group_ib.sdk и собирает контакты, SMS, журнал звонков.

Вывод: Т-Банк и MegaMarket — лидеры слежки с 65 из 68 обнаруженных проверок.

3. Неожиданные методы слежки

3.1. Чтение /proc/net/tcp — сканирование сетевых соединений ядра

Приложения: Т-Банк, Яндекс Браузер, Яндекс Карты, Yandex Music

Эти приложения читают файл `/proc/net/tcp` — таблицу TCP-соединений ядра Linux. Ищут порт `0x69A2` (27042) — стандартный порт Frida, инструмента реверс-инжиниринга. По сути, приложение проверяет, не анализирует ли кто-то его прямо сейчас. Это то, чего обычный пользователь никак не ожидает от банковского приложения или навигатора.

3.2. Тайминг нажатий на экран — поведенческая биометрия

Приложения (11): Т-Банк, Альфа-Банк, 2ГИС, Яндекс Еда, MegaMarket, Мой МТС, Одноклассники, Госуслуги, Rutube, Сбербанк Онлайн, Yandex Music

Перехватывают `dispatchTouchEvent()` — каждое касание экрана с координатами, давлением и временем. Сбербанк хранит объекты `TouchData` с полями `pressure`, `size`, `x`, `y`. Модуль com.group_ib.sdk (в Альфа-Банке, MegaMarket, Мой МТС) перехватывает все touch-события.

Почему это неожиданно: поведенческая биометрия позволяет идентифицировать человека по тому, *как* он нажимает на экран — даже

без логина. Rutube записывает координаты касаний, хотя это просто видеохостинг.

3.3. Детект Frida и Xposed — защита от реверс-инжиниринга

Приложения: Т-Банк, Яндекс Браузер, Yandex Music, Яндекс Карты

Ищут следы Frida (инструмент динамического анализа) через:

- Чтение `/proc/<pid>/maps` и поиск строки `frida`
- Проверка `/proc/net/tcp` на порт 27042

Почему это неожиданно: приложения активно противодействуют тому, чтобы пользователь или исследователь мог проанализировать, что они делают. Яндекс Карты — навигатор — защищается так, будто это военное ПО.

3.4. Список VPN-приложений — Самокат и MegaMarket

Приложения: Самокат, MegaMarket

Используют `queryIntentServices("android.net.VpnService")` — получают **список всех VPN-приложений**, установленных на устройстве. Не просто «включён ли VPN», а какие именно VPN-программы есть.

Почему это неожиданно: доставка еды (Самокат) и маркетплейс (MegaMarket) знают, какие VPN вы установили.

3.5. Детект Tor — Яндекс Браузер

Приложение: Яндекс Браузер

Единственное из 30 приложений, которое явно ищет пакеты Tor Browser: `org.torproject.torbrowser`, `org.torproject.torbrowser_alpha`.

Почему это неожиданно: браузер, который сам предлагает режим «Инкогнито», ищет инструмент анонимности на вашем устройстве.

3.6. Сканирование 200+ чужих приложений — Avito

Приложение: Avito

В блоке `<queries>` манифеста перечислено более 200 пакетов — банки (Сбербанк, Т-Банк, ВТБ, Альфа), маркетплейсы (Ozon, Wildberries), соцсети (VK, Telegram, Instagram, Facebook), сервисы (Яндекс), конкуренты (Drom, CIAN, HH.ru). Avito может определить, какие из этих приложений установлены.

3.7. Ozon знает, есть ли у вас AnyDesk и TeamViewer

Приложение: Ozon

Содержит захардкоженный маппинг: `com.anydesk.anydeskandroid` → `"AnyDesk"`, `com.teamviewer.quicksupport.market` → `"QS"`. Аналогичный список в Самокате. Приложения могут проверить наличие программ удалённого управления.

3.8. Тотальный fingerprinting устройств

29 из 30 приложений проверяют root-доступ (все кроме Яндекс Go). **24 из 30** проверяют, не подключён ли отладчик. **24 из 30** детектируют эмулятор.

Что это создаёт: уникальный «отпечаток» устройства, который позволяет отслеживать пользователя даже после переустановки приложения.

Трекерные SDK — кто за всеми следит

SDK	Количество приложений	Предположительный владелец
Yandex AppMetrica	17	Яндекс
MyTracker	14	VK (Mail.ru)
AppsFlyer	10	Израиль
Huawei HMS	9	Huawei (Китай)
Firebase Analytics	8	Google
Sentry	8	Sentry (США)
VK Push SDK	6	VK
SDK com.group_ib.sdk	3	Group-IB (Россия)

* ***Обновление от 16 апреля 2026 года:*** *представитель компании Group-IB сообщил команде RKS Global, что в апреле 2023 года Group-IB освободилась от своих активов и полностью ушла с российского рынка, и в настоящее время не обслуживает клиентов в России и не ведет там деятельность.*

Вывод: AppMetrica (Яндекс) и MyTracker (VK) — два главных российских трекера, встроенных в более чем половину проанализированных приложений. Данные с этих SDK доступны по запросу российских правоохранительных органов.

4. Какие разрешения работают без участия пользователя?

Android делит разрешения на два типа:

- **Dangerous (runtime)** — требуют явного согласия пользователя через всплывающее окно
- **Normal (install-time)** — предоставляются **автоматически** при установке APK, без какого-либо уведомления

4.1. «Тихие» разрешения — install-time (без согласия пользователя)

Эти разрешения формируют инфраструктуру слежки, которая **работает с момента установки**, ещё до того как пользователь нажмёт «Разрешить» хоть на что-нибудь:

Разрешение	**Приложений**	**Что это значит для пользователя**
RECEIVE_BOOT_COMPLETED	**30/30**	Приложение автоматически запускается при включении телефона
FOREGROUND_SERVICE	**30/30**	Приложение может работать постоянно в фоне
QUERY_ALL_PACKAGES / `<queries>`	**27/30**	Приложение видит **все** (или конкретные) установленные программы на устройстве

Разрешение	Приложений	Что это значит для пользователя
SYSTEM_ALERT_WINDOW	**16/30**	Приложение может рисовать поверх других приложений
FOREGROUND_SERVICE_DATA_SYNC	**15/30**	Фоновая синхронизация данных — канал для отправки собранного
REQUEST_INSTALL_PACKAGES	**15/30**	Приложение может устанавливать другие APK-файлы
REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	**12/30**	Система не может «усыпить» приложение — работает 24/7
FOREGROUND_SERVICE_MICROPHONE	**6/30**	Фоновый доступ к микрофону без видимого приложения
FOREGROUND_SERVICE_LOCATION	**4/30**	Непрерывная геолокация в фоне
FOREGROUND_SERVICE_MEDIA_PROJECTION	**4/30**	Захват экрана в фоне
FOREGROUND_SERVICE_CAMERA	**3/30**	Фоновый доступ к камере

Что это создаёт на практике: комбинация RECEIVE_BOOT_COMPLETED (все 30) + FOREGROUND_SERVICE (все 30) + REQUEST_IGNORE_BATTERY_OPTIMIZATIONS (12) = приложение запускается при каждом включении телефона, работает постоянно в фоне и не может быть остановлено системой экономии батареи. Вся эта инфраструктура ставится **без единого вопроса к пользователю**.

4.2. Разрешения, требующие согласия пользователя (dangerous/runtime)

Разрешение	Приложений	Что получает приложение
ACCESS_FINE_LOCATION	**30/30**	GPS-координаты с точностью до метров
CAMERA	**28/30**	Фото- и видеосъёмка
READ_CONTACTS	**28/30**	Полный список контактов
RECORD_AUDIO	**24/30**	Запись с микрофона
READ_MEDIA_IMAGES	**19/30**	Доступ к фотографиям
WRITE_EXTERNAL_STORAGE	**16/30**	Запись и изменение файлов
ACCESS_COARSE_LOCATION	**14/30**	Приблизительное местоположение
READ_CALL_LOG	**13/30**	Полная история звонков
ACCESS_BACKGROUND_LOCATION	**12/30**	Геолокация даже когда приложение закрыто
READ_MEDIA_VIDEO	**11/30**	Доступ к видеозаписям
WRITE_CONTACTS	**9/30**	Изменение контактов
READ_CALENDAR	**5/30**	Чтение событий календаря
READ_SMS	**5/30**	Чтение всех SMS-сообщений
RECEIVE_SMS	**4/30**	Перехват входящих SMS

Разрешение	Приложений	Что получает приложение
SEND_SMS	**1/30**	Отправка SMS без ведома пользователя

4.3. Рейтинг приложений по числу разрешений

Примечание: полные манифесты были доступны для 5 из 30 приложений (Т-Банк, VK Видео, Альфа-Банк, Яндекс Маркет, Яндекс Еда). Для остальных 25 подсчёт основан на упоминаниях разрешений в результатах анализа и является нижней оценкой — реальное число разрешений может быть выше.

#	Приложение	Dangerous (с согласием)	Normal (без согласия)	Всего
1	**Т-Банк (T-Bank)**	**23**	**24**	**47**
2	VK Видео	16	15	31
3	Альфа-Банк	13	17	30
4	Яндекс Маркет	12	14	26
5	Одноклассники	16	9	25
6	Яндекс Еда	10	14	24
7	MegaMarket	16	6	22
8	Сбербанк Онлайн	9	11	20
9	Avito	7	11	18
10	Яндекс Браузер	10	7	17
11	ВКонтакте	11	6	17
12	ВТБ Онлайн	11	6	17

#	Приложение	Dangerous (с согласием)	Normal (без согласия)	Всего
13	RuStore	10	7	17
14	2ГИС	9	7	16
15	Дзен	9	7	16
16	Мой МТС	7	8	15
17	Почта Mail.ru	10	5	15
18	Яндекс Go	7	8	15
19	MAX (TamTam)	9	5	14
20	Ozon	9	5	14
21	Кинопоиск	6	7	13
22	МегаФон	7	4	11
23	Yandex Music	7	4	11
24	Госуслуги	7	3	10
25	Mir Pay	3	6	9
26	Самокат	6	2	8
27	Wildberries	4	3	7
28	Яндекс Карты	4	3	7
29	Rutube	6	1	7
30	VK Music	?	?	?

Вывод: Т-Банк запрашивает 47 разрешений — больше всех. При этом 24 из них (включая автозапуск, фоновые сервисы камеры, микрофона, геолокации и установку APK) предоставляются **автоматически без ведома пользователя**. Банковские приложения (Т-Банк, Альфа-Банк,

Сбербанк) лидируют по числу «тихих» install-time разрешений, формирующих постоянную фоновую инфраструктуру.

Методология

- **Статический анализ:** декомпиляция через `apktool` и `jadx`, поиск по 68 проверкам в 12 категориях слежки
- **Ограничения:** только статический анализ, без динамического тестирования на устройстве
- **Оценка `check_failed`:** 3 из 2400 ячеек (0.12%) не удалось проверить — VPN-отправка у 3 приложений (Wildberries, Yandex Music, Яндекс Карты), где код скрыт в нативных библиотеках

Версии APK

Пакет	Версия
com.avito.android	v221.1
com.idamob.tinkoff.android	v7.31.1
com.vk.vkvideo	v1.139.1
com.vkontakte.android	v8.171
com.wildberries.ru	v7.5.6002-rustore
com.yandex.browser	v26.3.4.128
ru.alfabank.mobile.android	v12.46.05
ru.beru.android	v2026.10.2.c
ru.dublgis.dgismobile	v7.21.0.615.23
ru.foodfox.client	v3.120.0
ru.kinopoisk	v7.78.4
ru.mail.mailapp	v15.80.0.135859
ru.megafon.mlk	v4.63.0

Пакет	Версия
ru.megamarket.marketplace	v6.2
ru.mts.mymts	v6.63
ru.nspk.mirpay	v1.60.4.350
ru.ok.android	v26.3.30
ru.oneme.app	v26.11.3
ru.ozon.app.android	v19.11.0
ru.rostel	v25.2.0.9435-rustore
ru.rutube.app	v31.4.4-rustore
ru.sbcs.store	v3.227.0
ru.sberbankmobile	v17.4.0
ru.vk.store	v1.98.0.1
ru.vtb24.mobilebanking.android	v20.5.0.3
ru.yandex.music	v2026.03.4 #140rur
ru.yandex.taxi	v5.67.3
ru.yandex.yandexmaps	v28.4.3
ru.zen.android	v26.3.4
com.uma.musicvk	v8.19

Категории проверок (12 векторов слежки)

#	Вектор	Проверок
S1	Перечисление установленных приложений	6
S2	Детект VPN/Proxy/Tor	7
S3	Fingerprinting устройства (IMEI/IMSI/MAC)	7
S4	Отслеживание местоположения	5
S5	Мониторинг сети и телеметрия	5
S6	Доступ к контенту (контакты/SMS/файлы)	6
S7	Поведенческая аналитика (сенсоры/жесты)	6
S8	Аудио/видео наблюдение	4
S9	Скрытая экфильтрация данных	6
S10	Защита от анализа (root/Frida/эмулятор)	5
S11	Российский правовой контекст (СОРМ/Яровая)	4
S12	Системная персистентность	7
	Итого	**68**

Рекомендации

Часть 1. Вы в России

Модель угроз: данные, собранные приложениями, доступны ФСБ, МВД и СК — через СОРМ, закон Яровой и запросы к компаниям. Данные о VPN-приложении могут привести к его блокировке.

Изоляция приложений

24 из 30 приложений отправляют список ваших приложений на сервер. Если Сбербанк стоит рядом с VPN-клиентом — разработчики и силовики это знают.

- **Два телефона** — идеально. Один для российских приложений, второй для всего остального.
- **Один телефон** — Android Work Profile через Shelter. Приложения из разных профилей не видят друг друга: ни списка приложений, ни контактов, ни файлов. Work Profile не скрывает VPN — только данные между профилями, то есть он не помогает защищать VPN-приложения.

VPN

Решения (от лучшего к простому):

1. VPN на роутере. Туннель на роутере, телефон подключается по Wi-Fi. Роутер с OpenWrt / Keenetic / Mikrotik + WireGuard или VLESS. Портативный вариант — GL.iNet с VPN. Минус: только на Wi-Fi этого роутера.

1б. Раздача Wi-Fi с другого телефона. Тот же принцип, что VPN на роутере, но роутер — ваш второй телефон. На телефоне A включён VPN + мобильная точка доступа. Телефон B (с российскими приложениями)

подключается к Wi-Fi телефона А. Проверка: на телефоне В зайти на сайт определения IP — если показывает IP VPN-сервера, значит работает. Нюансы: не все VPN-клиенты маршрутизируют трафик хотспота через туннель, некоторые операторы ограничивают tethering, на Android 12+ бывают проблемы с маршрутизацией.

2. Два телефона. Телефон А с VPN — для браузера, мессенджеров, заблокированных сайтов. Телефон В без VPN — для российских приложений. На В нет VPN, потому что его там физически нет. Минус: два разных пространства для жизни.

3. Split tunneling (частичное решение). В некоторых VPN-клиентах можно исключить российские приложения из туннеля. Их трафик идёт напрямую, но `tun0` на устройстве остаётся. Минус: Помогает против части проверок, но приложения, сканирующие `tun0`, всё равно увидят VPN.

4. Переключение. Выключить VPN → открыть приложение → принудительно остановить приложение (Настройки → Приложения → Остановить) → включить VPN. Важно именно остановить, а не просто свернуть: все 30 приложений работают в фоне и могут зафиксировать момент включения VPN. Минус: нужно всё помнить.

Разрешения — отозвать сейчас

Разрешение	**Действие**
Геолокация	Только навигаторам, только «при использовании».
Контакты	Отозвать у всех кроме мессенджеров
Микрофон, камера	Только по запросу.
Журнал звонков, SMS	Отозвать у всех.

Фоновая активность

Все 30 приложений автозапускаются и работают в фоне. Ограничить: Настройки → Приложения → Батарея → «Ограничено». Не разрешать обход оптимизации батареи.

Перейти на iPhone

Весь отчёт — про Android. На iOS большинство описанных методов слежки невозможны. Что остаётся на iOS: геолокация (если дали разрешение), контакты (если дали), камера/микрофон (если дали), VPN-детект через `utun` (частично), поведенческая аналитика через SDK. Но объём слежки радикально меньше — из 68 проверок отчёта на iOS реализуемы ~20–25. А если на iPhone включить Lockdown mode, то ещё меньше.

Важный нюанс: iPhone не раздаёт VPN через хотспот. В отличие от Android, где VPN маршрутизирует трафик хотспота через туннель, на iOS Personal Hotspot отправляет трафик подключённых устройств напрямую в сотовую сеть, минуя VPN. Для раздачи VPN используйте Android-телефон или роутер.

Прочее

Буфер обмена: Wildberries перехватывает в фоне. Используйте менеджер паролей с автозаполнением.

Часть 2. Вы уехали из РФ

Модель угрозы: российские серверы узнают, где вы живёте, через IP-адрес, GPS, список приложений, контакты, SIM-роуминг и часовой пояс.

Изоляция — обязательна

Если на одном телефоне рядом со Сбербанком стоят иностранные приложения — любое из таких приложений, отправляющих список установленных программ на сервер, выдаёт вашу страну.

- **Два телефона** — лучший вариант. Старый iPhone только для российских приложений.
- **Один телефон** — Work Profile (Shelter) обязателен. Российские приложения не видят список приложений из основного профиля.

Отлично на телефоне для российских приложений держать включенным российский VPN, так как открытый IP показывает вашу примерную геолокацию. Также местонахождение утекает через: GPS, сотовые вышки (российский оператор через роуминг), список приложений (местные сервисы), часовой пояс устройства. Каждый канал отлично закрывать отдельно.

Геолокация

Отозвать у **всех** российских приложений. Навигация за рубежом — Google Maps / OsmAnd. Если нужен Яндекс Go — только при использовании.

Контакты

Отозвать у всех российских приложений. За рубежом у вас контакты местных людей и организаций.

SIM-карта

Российская SIM за рубежом — оператор видит роуминг. Перевести в режим «только для SMS» (подтверждение банков). Основная связь — местная SIM. Идеально: российская SIM в российском телефоне, основная (местная зарубежная) – в основном.

Обновление от 16 апреля 2026: повторный анализ 30-ти популярных российских приложений

Методология

По сообщениям СМИ, Минцифры России установило 15 апреля как ожидаемую дату для введения ограничений для пользователей с включенными VPN. Ограничения должны реализовывать популярные российские онлайн-магазины и интернет-ресурсы — в том числе через приложения.

Исследователи RKS Global сделали повторный анализ тех же 30-ти приложений, которые рассматривались ранее. Были получены обновлённые версии APK (26 из 30 обновились между 7 и 16 апреля). Метод исследования — статический анализ APK (декомпиляция через apktool + jadx, анализ нативных библиотек, расшифровка XOR-обфусцированных строк) плюс динамическое тестирование на устройстве: Pixel 7a, Android 16, Magisk root, frida-server; VPN — AmneziaVPN (WireGuard, интерфейс `tun0`); запуск каждого приложения на 15 секунд, capture `adb logcat -d`, сравнение VPN ON vs VPN OFF.

Ключевые результаты

Все 30 из 30 приложений детектируют VPN (при первом анализе было 22 из 30). 20 из 30 активно блокируют или ограничивают функционал при обнаружении VPN. Семь приложений получают полный список

установленных VPN-клиентов. Число обнаруженных методов VPN-детекции выросло с 6 до 10: к прежним (`hasTransport`, сканирование интерфейсов, `/proc/net/tcp`, proxy-настройки, детект Tor, передача на сервер) добавились полноэкранная UI-блокировка, VPN app enumeration через `queryIntentServices`, вероятностная модель с весами, эвристика MTU <1400.

Список установленных VPN-клиентов

Семь приложений — Wildberries, 2ГИС, МТС, Ozon, Мегамаркет, RuStore, Одноклассники — получают полный список VPN-клиентов через системный вызов `queryIntentServices("android.net.VpnService")`, возвращающий названия всех установленных VPN-приложений (AmneziaVPN, WireGuard, OpenVPN, NordVPN и т.д.).

В пяти из семи список передаётся через антифрод-SDK BI.ZONE вместе с 77 другими параметрами устройства. В манифесте каждого из семи приложений присутствует блок `<queries><intent><action android:name="android.net.VpnService"/></intent></queries>`.

Централизация VPN-слежки в экосистемах

Все семь приложений Яндекса (Браузер, Карты, Маркет, Еда, Кинопоиск, Музыка, Go) используют единый Yandex Passport SDK с `CheckVpnStatusUseCase`, POST-запросом к `mobileproxy.passport.yandex.net/tmgrdfrend/checkvpn` (с GPS, регионом SIM-карты и device ID в payload) и полноэкранной блокировкой `VpnChallengeActivity` при отказе. Серверный флаг `android_block_vpn` позволяет дистанционно включать блокировку в любом из семи приложений; механизм `VpnStatusChangedCommand` обеспечивает IPC-обмен VPN-статусом между ними на одном устройстве.

Почта Mail.ru (`VpnProbabilityConnectivityChecker`) и Дзен (модуль `ru.zen.zapret`) реализовали идентичную вероятностную модель: пять сигналов (`hasTransport`, interface scan, proxy, MTU <1400 и др.) с двумя весовыми таблицами (cellular/WiFi) и четырьмя уровнями уверенности. Сбербанк через Kaspersky SDK использует 11-позиционный enum `com.kavsdk.internal.wifi.VpnClientStatus` — от `VpnClientUnavailable` через установку, запуск, активность, отключение до автоматического переподключения.

Динамическое тестирование

У Яндекс Go за 15 секунд при включённом VPN зафиксировано 77 logcat-событий против 39 без VPN; AppMetrica логирует `isVpn:true` в каждом сетевом событии:

AppMetrica: [ru.yandex.taxi] Event received: Network.Proxy.
With value: {networkType=wifi, isVpn=true, duration=0,
url=https://mob-manager-aws.mob.taxi.yandex.net/, type=DIRECT}

У 2ГИС в logcat — прямой текст детекции и обращения к выделенному endpoint:

Grym/DeviceState: [VPN] Detected via TRANSPORT_VPN

За 15 секунд — четыре обращения к `relay-api.eu.2gis.com/v1/vpn-detection-free`. У Яндекс Еды сервер при включённом VPN возвращает `checkVpnStatusUseCase Allowed false` — приложение блокирует доступ.

Обфускация VPN-детекции в MAX

В мессенджере MAX (DPS SDK, пакет `ru.trace_flow.dps`) имена сетевых интерфейсов (`tun`, `ppp`, `tap`, `pptp0`) закодированы XOR-ключом `0xDE60D9E8` и раскрываются в runtime. SDK обращается к шести hardcoded IP-check endpoints (`api.ipify.org`, `checkip.amazonaws.com`, `ifconfig.me`, `ip.mail.ru`, `ipv4/ipv6-internet.yandex.net`) для сравнения реального IP и VPN IP — единственный случай среди 30 приложений. Четыре канала эксфильтрации VPN-флага: `trace-flow.ru/api/v1/report`, `api.oneme.ru`, `vk-analytics.ru`, `apptracer.ru`.

Корректировка рекомендаций

1. **Split tunneling** (исключение российских приложений из VPN-туннеля, предлагался в первой версии как частичное решение) **недостаточен против новых методов детекции.**

Тринадцать приложений сканируют сетевые интерфейсы через `NetworkInterface.getNetworkInterfaces()` — этот API возвращает `tun0` любому приложению независимо от маршрутизации, потому что Android не изолирует network namespace по процессам. Семь приложений через `queryIntentServices` получают список установленных VPN-клиентов — метод проверяет PackageManager, а не сетевой стек. Mail.ru и Дзен включают в вероятностную модель эвристику MTU <1400, срабатывающую на `tun0` независимо от того, исключено ли приложение из туннеля. Два приложения читают `/proc/net/tcp` — глобальную таблицу ядра, доступную всем процессам.

2. **VPN на роутере остаётся эффективным**. При подключении телефона по Wi-Fi к роутеру с VPN на устройстве не создаётся `tun0`, не меняется MTU и не активируется VPN-транспорт на уровне Android API. Все 10 обнаруженных методов детекции работают на уровне сетевого стека устройства — при туннелировании на уровне роутера они не срабатывают.

3. **Android Work Profile (Shelter) из «дополнительной меры» становится критической мерой из-за VPN app enumeration**. Если VPN-клиент установлен в том же профиле, что и одно из семи приложений, использующих `queryIntentServices` (Wildberries, Ozon, МТС, Мегамаркет, RuStore, 2ГИС, Одноклассники), — они получат его имя пакета и передадут на сервер через антифрод-SDK.

Благодарим сообщество за интерес к нашей работе, поддержку и критику наших идей. Мы призываем обмениваться данными, развивать и наращивать нашу общую экспертизу.
Если у вас есть вопросы или предложения для технической команды, пишите на tech@rks.global.