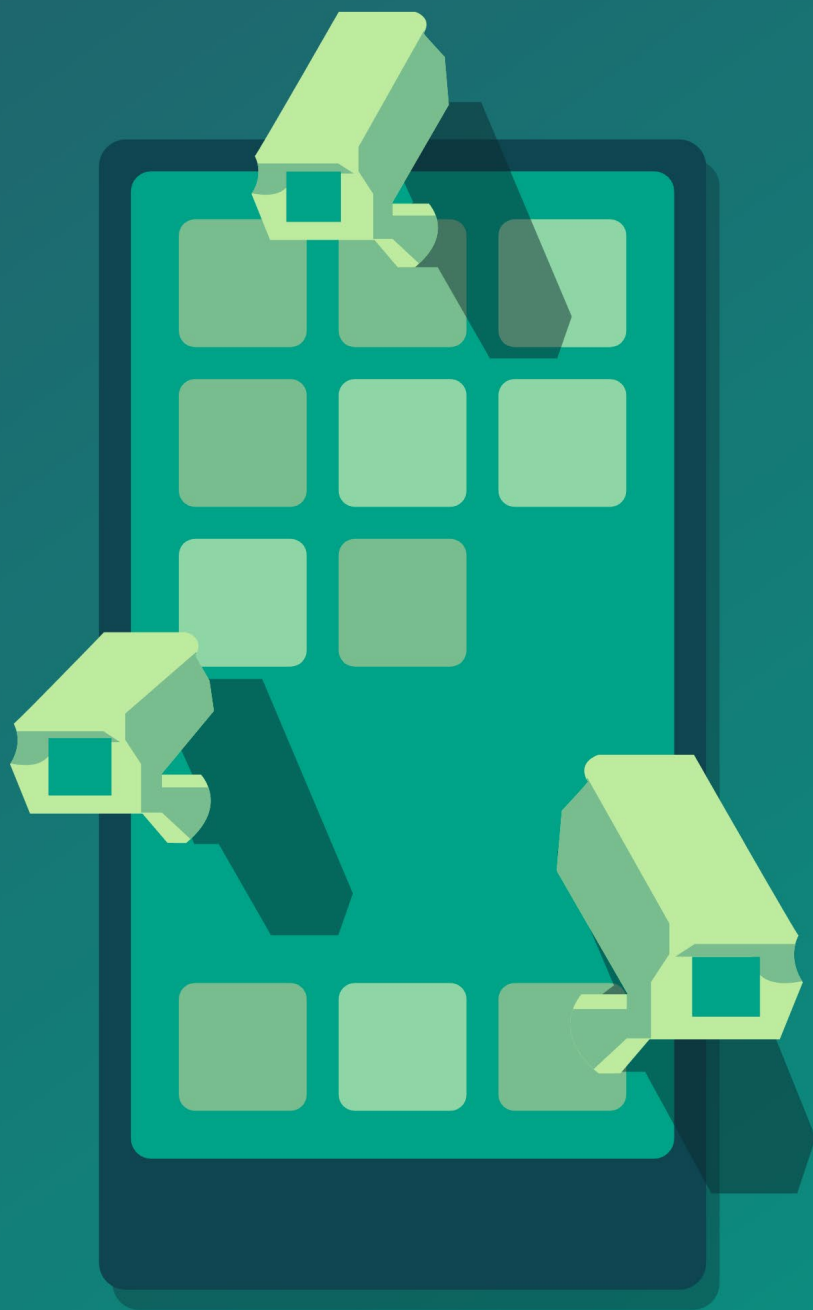




Приватность мобильных приложений магазина RuStore



Информационная
культура

**Авторы: Иван Бегтин, Василий Буров,
Ксения Орлова**

АНО «Информационная культура»

infoculture.ru

infoculture@infoculture.ru

telegram.me/infoculture

youtube.com/infoculture

twitter.com/InfocultureRu



Оглавление

Введение	3
Резюме.....	6
Трекеры.....	6
Разрешения.....	8
Выводы.....	9
Методика исследования	12
Ключевые вопросы исследования	12
Алгоритм сбора данных.....	12
Принципы формирования результатов	14
Данные	15
Результаты анализа	16
Трекеры.....	16
Приложения без трекеров	18
Какими бывают трекеры	19
Какие трекеры чаще всего установлены в приложениях.....	21
Категории приложений и число трекеров	23
Приложения с большим числом трекеров	26
Юрисдикции и компании	29
Компании-авторы трекеров	33
Приложения и трекеры компаний «Яндекс» и VK	37
Разрешения.....	47
Рекомендации.....	53

Введение

Повсеместное распространение смартфонов и растущее использование интернета способствуют росту рынка мобильных приложений по всему миру. Многие действия стало привычно выполнять именно с мобильного: будь то взаимодействие с банком, общение в социальных сетях или обращение за государственными услугами. Две глобальные цифровые экосистемы компаний Apple (iOS) и Google (Android) стали постоянным спутником практически любого гражданина в его повседневных делах.

И это привлекает внимание к вопросам приватности мобильных приложений. Ведь многие из них благодаря встроенным системам-трекерам могут отслеживать действия пользователей или имеют такие разрешения на смартфоне, которые дают им доступ как к хранящейся информации, так и возможностям доступа к звонкам или камере и микрофону – причем, далеко не всегда оправданными функционалом приложения.

В последние годы в мире растет число проводимых по этой теме исследований. В первую очередь они касаются приложений для операционной системы Android – что продиктовано в первую очередь тем, что iOS является закрытой мобильной платформой, что значит существует множество сложно преодолимых барьеров, затрудняющих сбор данных и анализ приложений. В то же время платформа Android, напротив, является более открытой и доступна для разных методик и инструментов, позволяющих проводить исследования приложений.

Например, проект Exodus Privacy обеспечивает мониторинг наличия критичных разрешений и программ-трекеров, следящего кода передающего личные данные другим компаниям, внутри приложений для

Android¹. В проекте Privacy not included² от Mozilla Foundation исследователи вручную, по предварительно разработанной методике, оценивают степень приватности и безопасности мобильных приложений, а также наличие в них технологий ИИ, возможно, используемых против интересов пользователей.

Эти проекты решают важную задачу **повышения осведомлённости** пользователей мобильных устройств и помогают в выборе между приложениями обеспечивающими меньшую и большую приватность при выполнении одинаковых функций. Большая осведомленность и позволяет вести диалог с регуляторами, владельцами магазинов приложений и разработчиками приложений по повышению приватности мобильных приложений, снижению объёмов передаваемых данных и сокращению числа случаев наиболее недружественных к пользователям практик.

Особого внимания требуют мобильные приложения, создаваемые органами государственной власти, которые используются гражданами безальтернативно. Например, прошлом году нами было проведено исследование 44 приложений, разрабатываемых органами власти и опубликованных в магазине приложений Google Play³. Оно показало, что во многих государственных приложениях содержится код специальных отслеживающих трекеров. И это не какие-то внутригосударственные системы, а передача данных об использовании приложений пользователями сторонним лицам, в первую очередь глобальным bigtech-компаниям — Google и Meta*⁴.

В новом исследовании мы решили проверить приложения, которые размещены не Google Play, самом главном магазине приложений для Android, а в новом российском магазине приложений RuStore

¹ <https://exodus-privacy.org>

² <https://foundation.mozilla.org/en/privacynotincluded/>

³ <https://privacygismobapps.infoculture.ru/>

⁴ * Суд признал экстремистской компанию Meta и запретил в России деятельность корпорации по реализации социальных сетей Facebook и Instagram.

(<https://rustore.ru>). Из-за возникших после февраля 2024 года санкционных ограничений, в том числе касающихся размещения некоторых важных для пользователей приложений (например, банковских) в Google Play, стали актуальны альтернативные магазины приложений, и на роль главного из них претендует именно RuStore, который Минцифры России рекомендует для предустановки на продаваемые смартфоны⁵. Магазин создан и поддерживается компанией VK (ранее известной как Mail.ru). К тому же, Правительство РФ определило VK единственной организацией, «обеспечивающей создание и функционирование единого магазина приложений, применяемых потребителем с использованием технически сложных товаров».⁶

Фокус исследования: как мобильные приложения соблюдают приватность пользователя с точки зрения передачи данных третьим лицам через встроенные трекеры и наличие разрешений, запрашиваемых приложением, и того, насколько эти разрешения могут использоваться в целях сбора данных.

⁵ https://www.rbc.ru/technology_and_media/18/05/2022/6284c8b69a794762883c5690

⁶ <http://publication.pravo.gov.ru/Document/View/0001202208160022>

Резюме

В рамках исследования были собраны данные о 1014 мобильных приложениях, опубликованных в официальном и рекомендованном для предустановки на продаваемые смартфоны магазине RuStore, которые были там доступны для установки на 28 июля 2022 года. Из них было отобрано для исследования **934 приложения** (подробнее в разделе «Методика исследования»).

Проведенный анализ показал наличие в них 106 различных встроенных сторонних — то есть не имеющих отношения к их разработчикам — трекеров (trackers), а также использование 602 уникальных разрешений (permissions) для доступа к данным и функциям устройства.

Трекеры

Трекеры — это встраиваемые в код мобильных приложений модули, которые используются для сбора информации, отслеживая работу приложения или поведение пользователей. Это к примеру: аналитические метрики, сбор данных об ошибках и сбоях, оценка производительности и прочее. Трекер обычно распространяется компаниями в виде SDK (Software Development Kit) — готового набора инструментов, призванного облегчить работу разработчиков приложений. В рамках этого анализа мы также отнесли к этой категории модули, обеспечивающие авторизацию через социальные сети, опираясь на то, что они тоже могут передавать чувствительную информацию.

- Было обнаружено 114 приложения (12%), которые не содержат ни одного трекера в коде.
- Из 106 найденных в приложениях трекеров 46 (43,4%) являются рекламными. 18 трекеров (17%) используются для профайлинга пользователей и 8 трекеров используется для идентификации пользователя.
- Было обнаружено, что для приложений, имеющих как минимум один отслеживающий трекер, а таких 820 (87,8%), характерно следующее:
 1. Чаще всего в них установлены трекеры компании Google: Google Firebase Analytics — 699 приложений (85,2%), Google CrashLytics — 449 приложений (54,8%). И третий по популярности — российский трекер AppMetrica от компании «Яндекс» — 407 приложений (49,6%).
 2. Подавляющее большинство приложений (776 ед. или 94,6%) имеют встроенные сторонние трекеры, принадлежащие иностранным юрисдикциям.
 3. По числу приложений, юрисдикциям которых принадлежат трекеры, лидируют: США, Россия и Китай. В 769 (93,8%) таких приложениях используются трекеры, принадлежащие компаниям юрисдикции США.
 4. Среди компаний, ожидаемо, лидируют трекеры: Google — 744 приложения (90,7%), «Яндекс» — 407 приложений (49,6%) и Meta — 204 приложения (24,9%).
 5. 401 приложение (48,9%) имеет трекеры, принадлежащие как минимум 3 компаниям и больше.
 6. Российские трекеры, в основном принадлежащие компаниям «Яндекс» и VK, используются в 477 (58%) приложениях. Часто они используются наряду с другими иностранными трекерами, выполняющими аналогичные функции.

Всего в 44 приложениях (5,3%) установлены только российские трекеры, без соседства с трекерами иных юрисдикций.

- Приложения категорий «Игры» и «Развлечения» являются наиболее нагруженными трекерами. Большая часть таких приложений относятся к категориям «Игры» и «Развлечения». Это говорит о том, что несмотря на бесплатность представленных приложений, пользователь платит собственными данными, предоставляя с помощью приложения к ним доступ многочисленным компаниям, которым принадлежат установленные трекеры.
- Код трекеров, в том числе компаний в зарубежных юрисдикциях содержится, в том числе в мобильных приложениях, созданных госорганами. Несмотря на то что их меньше чем в других категориях приложений (медианное значение составляет всего 2,5 трекера на приложение), тем не менее, в отличие от других приложений, государственные приложения являются безальтернативными.

В отношении трекеров созданных органами власти нашей командой в 2021 году проводилось исследование, в котором подробно рассматривались государственные мобильные приложения⁷. С момента публикации этого исследования никаких качественных изменений в госполитике в этой области не произошло.

Разрешения

Разрешения — это права доступа, которые приложение запрашивает для доступа к телефону. Они могут касаться различных функций или частей информации, например, доступа к геолокации, контактам, файлам, микрофону, функции вибрации, камере и так далее.

⁷ <https://privacygsmobapps.infoculture.ru/>

Среди 934 исследованных приложений было обнаружено 602 уникальных разрешения, из которых 19 относятся к потенциально опасным, согласно списку уровней защиты для Android от Google⁸.

- Большинство приложений (821 единица или 88%) приложений запрашивает как минимум одно потенциально опасное разрешение.
- Только в 176 (18,8%) приложениях не обнаружено потенциально опасных разрешений.
- Всего в 17 приложениях (1,8%) нет ни одного разрешения к функциям и данным устройства, а также нет ни одного установленного трекера.
- Из потенциально опасных разрешений в приложениях чаще всего встречаются: доступ на чтение и запись во внешнее хранилище данных, доступ к камере, доступ к точному и приблизительному местоположению, получению информации об устройстве и записи аудио.
- Из 29 приложений таблице 14 «Приложения, в которых установлено 10 и более опасных разрешений», 10 — принадлежат компании VK.
- Больше всего таких разрешений запрашивают приложения «VK Звонки: безлимитное общение» (14), «Одноклассники: социальная сеть» (14), «ICQ - видеозвонки, чаты» (13), которые принадлежат компании VK.

Выводы

По итогам проведённого нами анализа можно утверждать, что несмотря на то, что RuStore имеет статус официального российского магазина приложений, большая часть опубликованных там приложений передают

⁸ <https://developer.android.com/guide/topics/permissions/overview>

данные в компаниям, находящимся в зарубежных юрисдикциях, которые, по мнению Правительства РФ, считаются недружественными странами^{9,10}.

Также можно обратить внимание, что запуск RuStore как замены существующему официальному магазину приложений для Android такому, как Google Play, снижает возможности пользователей по контролю приватности и осознанному выбору приложений из нескольких альтернатив. В отличие от Google Play, в RuStore отсутствует обязательное раскрытие разработчиками обязательств по соблюдению приватности, так называемого блока Data Safety¹¹, а также отсутствует практика раскрытия кода, как это делается в каталоге приложений F-Droid¹².

На сегодняшний день требования к приватности не закреплены ни в формальных требованиях к магазину приложений RuStore, ни в форме добровольной декларации от руководства оператора магазина — компании VK.

Официальный статус магазина приложений RuStore и признание VK его оператором в распоряжении Правительства РФ¹³ означают ответственность Правительства РФ, наравне с группой VK и разработчиками мобильных приложений, за передачу личных данных пользователей третьим лицам. В первую очередь это касается глобальных

⁹ Перечень недружественных России стран и территорий Распоряжение от 5 марта 2022 года №430-р: <http://government.ru/news/44745/>

¹⁰ Распоряжение от 20 июля 2022 года №1998-р о расширении перечня недружественных России стран: <http://government.ru/news/46080/>

¹¹ https://support.google.com/googleplay/answer/11416267?hl=en&visit_id=637964159138108522-1798468820&p=data-safety&rd=1

¹² <https://f-droid.org/ru/>

¹³ Распоряжение Правительства Российской Федерации от 13.08.2022 № 2235-р <http://publication.pravo.gov.ru/Document/View/0001202208160022>

Big Tech корпораций, чьи технологии наиболее явно используются в рынке «надзорного капитализма»¹⁴.

Ситуация усложняется тем, что органы государственной власти выступают не только регуляторами, но и заказчиками и разработчиками мобильных приложений, которые, как выясняется, также содержат код передачи пользовательских данных компаниям BigTech и иным зарубежным и российским компаниям. Подобная практика обесценивает политические декларации о защите данных и интересов граждан и вызывает вопросы к претензиям со стороны этих же государственных структур к коммерческим компаниям.

На сегодняшний день государство не только не выступает в роли регулятора, защищающего приватность граждан, но и не имеет средне- и даже краткосрочной стратегии в регулировании разработки собственных мобильных приложений.

Необходимы специальные требования и стандарты разработки государственных мобильных приложений, а также включение типовых положений по контролю приватности в технические задания для государственных закупок по 44-ФЗ и 223-ФЗ и корпоративных нужд.

Подробные рекомендации приведены в одноименном разделе этого документа.

¹⁴ <https://www.iep.ru/ru/izdatelstvo/book/2022/epokha-nadzornogo-kapitalizma-bitva-za-chelovecheskoe-budushchee-na-novykh-rubezhakh-vlasti-.html>

Методика исследования

Ключевые вопросы исследования

1. Какие трекеры чаще всего используются внутри приложений?
2. Какие компании владеют трекерами, которые собирают и передают данные из приложений?
3. В каких юрисдикциях базируются компании — издатели трекеров?
4. Какие разрешения, в том числе потенциально опасные, используются в приложении для его работы?

Алгоритм сбора данных

1. Были собраны данные о всех 1014 мобильных приложениях, опубликованных в RuStore — российском магазине мобильных приложений для Android. Приложения были собраны в виде данных APK файлов (Android Package) мобильных приложений, а также были собраны их основные характеристики (метаданные) приложения в магазине приложений RuStore. Эти характеристики включают:
 - название
 - описание
 - компания-разработчик приложения
 - категория приложения (см Таблица 1.).
 - и другие характеристики.

Путь сплошного анализа, помимо относительно небольшого объема размещенных приложений, был выбран в связи с ограничением магазина RuStore: он не предоставляет сведений о количестве установок приложений. Это делает невозможным проведение ранжирования или формирования выборки по самым популярным приложениям.

Таблица 1. Список категорий приложений в RuStore и число приложений в них.

Категория	Число приложений
Инструменты	192
Игры	176
Образование	165
Финансы	139
Развлечения	120
Социальные	90
Транспорт	83
Покупки	57
Здоровье и спорт	55
Государственные	45
Объявления и услуги	43
Новости	38
Еда и напитки	32
Медицина	29
Детские	3

В полученном наборе приложений была обнаружена аномалия – размещение 81 типового приложения, созданных ООО «Новатор». Это идентичные приложения логопедического назначения, каждое из которых соответствует определенному звуку языка. Все эти приложения, согласно категоризации в магазине RuStore, записаны как образовательные и игровые. Если бы мы оставили их все, то при

анализе бы получили фактическое искажение результатов, поэтому в расчете показателей оставили только одно, исключив остальные 80.

Таким образом, в итоговом списке осталось **934 приложений**.

2. По каждому приложению были собраны сведения о запрашиваемых приложением специальных разрешениях (permissions) и используемом коде сторонних отслеживающих мобильных трекеров. Для этого использовалась база [Exodus Privacy](https://exodus-privacy.eu.org/en/)¹⁵. Это некоммерческий проект по идентификации трекеров и разрешений в мобильных приложениях. Он включает большую базу уже проверенных приложений для Android, базу отпечатков ETIP¹⁶. Сведения, извлекаемые из APK файлов приложений с помощью статического анализа. Статический анализ включает проверку наличия java-классов в DEX файлах приложений на соответствие базе отпечатков мобильных трекеров.

Принципы формирования результатов

При подготовке данных использовался автоматизированный метод сбора данных о мобильных приложениях, который включает загрузку метаданных о трекерах с портала [Exodus Privacy](https://exodus-privacy.eu.org/en/). С помощью базы трекеров для каждого приложения, выгруженного из Rustore, записаны следующие данные:

- Наименование компании владельца/ разработчика трекера;
- Страна, в юрисдикции которой находится владелец/ разработчик трекера.

¹⁵ <https://exodus-privacy.eu.org/en/>

¹⁶ <https://etip.exodus-privacy.eu.org/>

- Описание и категория трекера по типу использования.

Недостающие данные в описаниях трекеров (компания-разработчик, юрисдикция) дополнялись вручную на основе общедоступной информации, опубликованной на веб-сайте трекера или компании-издателя трекера. Юрисдикции были определены по местонахождению компании-владельца (штаб-квартире) трекера и юрисдикции.

Итоговые данные сводились с помощью написанных скриптов на языке Python и были перепроверены вручную.

Данные

- Исходный код и данные опубликованы в репозитории:
<https://github.com/infoculture/rustore-privacy>.
- Данные содержатся в папке [export](#).

Результаты анализа

Трекеры

Трекеры — это встраиваемые в код мобильных приложений модули, которые используются для сбора информации, отслеживая работу приложения или поведение пользователей. Это к примеру: аналитические метрики, сбор данных об ошибках и сбоях, оценка производительности и прочее. Трекер обычно распространяется компаниями в виде SDK (Software Development Kit) — готового набора инструментов, призванного облегчить работу разработчиков приложений. В рамках этого анализа мы также отнесли к этой категории модули, обеспечивающие авторизацию через социальные сети, опираясь на то, что они тоже могут передавать чувствительную информацию.

Код трекера получает доступ к данным мобильного устройства, агрегирует их и передает вовне пользовательского устройства для хранения в базе данных и построения аналитики. Такие хранилища как правило находятся на стороне стороннего лица – компании-разработчика трекера, не контролируемого ни пользователем, ни разработчиком приложения. Основное назначение трекеров – давать разработчикам представление о том, как используется приложение. А это значит, что трекеры могут использоваться для скрытого сбора данных, а затем и для перепродажи данных на рекламном рынке. Для явного обнаружения скрытой передачи данных и конечных получателей данных необходимы технические испытания с трафиком, который генерирует приложение.

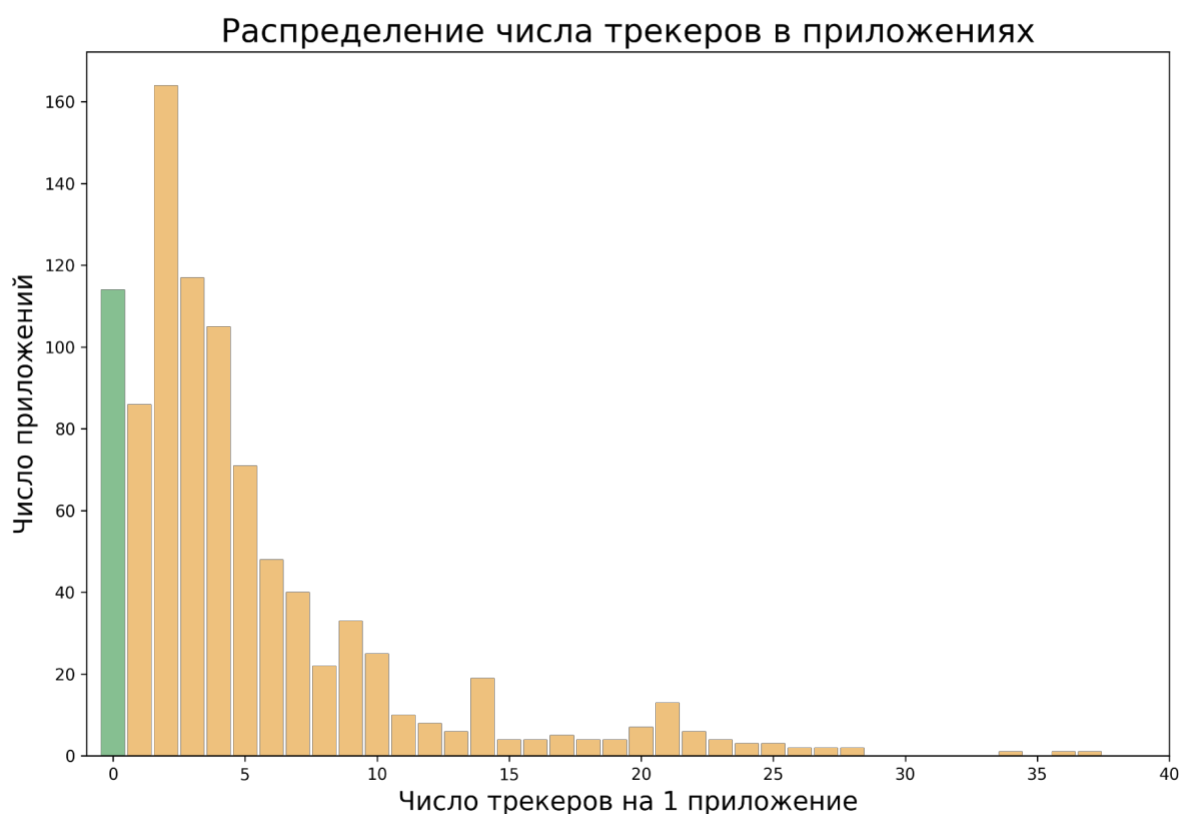


Диаграмма 1. Распределение числа трекеров в приложениях.

Основные выводы по распределению числа трекеров в приложениях:

1. Только 12% (114) приложений не имеют ни одного трекера.
2. Чаще всего встречаются приложения с 2 трекерами. Это 164 приложений или 17,5%.
3. Содержат от 1 до 5 трекеров 58% (543) приложений.
4. Около 30% (277) приложений имеют более 5 трекеров.

Далее рассмотрим приложения с нулевым количеством трекеров, а в подразделе **«Приложения с большим числом трекеров»** — наиболее нагруженные трекерами приложения.

Приложения без трекеров

Было обнаружено 114 приложения (12%), которые не содержат ни одного трекера в коде.

Некоторые другие примеры приложений без трекеров: Чат знакомств Galaxy, Lenta.ru, Рамблер/гороскопы, приложение «Цифровая школа Оренбуржья» Министерства цифрового развития и связи Оренбургской области, приложение «Господдержка АПК НСО» Министерства цифрового развития и связи Новосибирской области.

Приложений, которые не запрашивают ни одного разрешения и не имеют ни одного трекера в коде, было обнаружено всего 17 (1,8%) из 934 и все они относятся к разным тематическим категориям приложений: образование, финансы, игры и развлечения, транспорт, новости и др. Это не позволяет сформулировать вывод о том, что приложения определенных категорий являются наиболее безопасными с точки зрения полного отсутствия в них сторонних отслеживающих трекеров и разрешений, в т.ч. потенциально опасных. Однако даже в этом случае сами приложения могут самостоятельно собирать данные пользователей и продавать их на рекламном рынке. Особенно это касается развлекательных бесплатных приложений.

Подробнее о том, что такое разрешения, запрашиваемые мобильным приложением, и почему они могут быть потенциально опасными, читайте в разделе **«Разрешения»**.

Таблица 2. Список приложений, которые не запрашивают ни одного разрешения и не имеют ни одного трекера в коде.

Приложение	Компания-публикатор приложения	Категория
FOODUFA	ООО "ИНФОКРУГ"	Еда и напитки
Курить, чтобы бросить!	ООО "ЭргоСоло"	Здоровье и спорт
2048 + 15	Anton Bezdolny	Игры
БУКВА	Anton Bezdolny	Игры
Нашарик	Viktor Trofimov	Игры
Открой дверь. Квест для детей	ИП Фонов Дмитрий Владиславович	Игры, Образование
Трудодень	Камалов Роман	Инструменты
Lenta.ru	Лента.py	Новости
Спряжения глаголов	Nesmit School	Образование
Умный кролик	CatDonut	Образование
Суффиксы причастий	Nesmit School	Образование
Zen Relax - Антистресс	Viktor Trofimov	Развлечения
Рамблер/гороскопы	РАМБЛЕР ИНТЕРНЕТ ХОЛДИНГ	Развлечения
Штрафы ГИБДД: проверка и оплата	ООО ПЛАТИУСЛУГИ"	Транспорт
Топливный калькулятор	KB2soft	Транспорт
Оплата кредитов	ООО "ПЛАТИУСЛУГИ"	Финансы
Оплата ЖКХ ПлатиУслуги.py	ООО "ПЛАТИУСЛУГИ"	Финансы

Какими бывают трекеры

Прежде чем подробнее описывать, какие трекеры чаще всего используются в приложениях и в каких приложениях содержится наибольшее количество, рассмотрим распределение числа используемых трекеров по типам с точки зрения целей их использования.

Среди всех приложений обнаружено всего 106 уникальных трекеров. Согласно сведениям, собранным из базы Exodus Privacy, они относятся к **8 типам** по цели их использования (Таблица 3). А некоторые из них могут одновременно принадлежать сразу к нескольким типам. Например, таким является трекер Segment, который собирает сведения о поведении

пользователей. В базе Exodus Privacy он размечен одновременно как аналитический и профилирующий¹⁷. Другие подобные примеры трекеров представлены в **таблице 4. «Какие трекеры чаще всего установлены в приложениях»**.

Более половины (57 трекеров или 53,8%) трекеров относится к аналитическим. Рекламными являются 43,4% (46 трекеров) трекеров. Для профайлинга пользователей используются 17% (18 трекеров), и 16% (17 трекеров) – для сбора информации о местоположении устройства. Подробнее смотрите в Таблице 3. «Типы трекеров».

Таблица 3. Типы трекеров¹⁸.

Тип трекера	Описание	Число трекеров
Аналитика	Эти трекеры предназначены для сбора данных об использовании приложения и позволяют разработчику лучше узнать свою аудиторию. Например, узнать, какую страницу чаще всего посещают пользователи, или как долго они остаются на определенном участке страницы.	57
Реклама	Эти трекеры нацелены на идентификацию пользователя приложения для того, чтобы подавать ему целевые рекламные объявления. Цель создателя такого трекера — монетизировать свое приложение, т.е. заработать деньги с помощью рекламы.	46
Геолокация	Эти трекеры предназначены для определения географического положения мобильного устройства. Для этого данный тип трекеров использует преимущества нескольких датчиков: GPS-чипы, окружающие вышки сотовой связи, Wi-Fi сети, присутствующие в районе, близлежащие Bluetooth-сигналы и др.	18
Профайлинг	Цель этих трекеров — собрать как можно больше информации о пользователе приложения, чтобы построить виртуальный профиль. С этой целью трекер, например, обращает внимание на историю просмотров, список установленных приложений и т. д.	17

¹⁷ <https://etip.exodus-privacy.eu.org/trackers/c1d2096d-0d88-4a11-9728-1dbfc1e6c071/>

¹⁸ <https://reports.exodus-privacy.eu.org/en/info/trackers/>

Идентификация	Эти трекеры отвечают за определение вашей цифровой идентичности. Эта идентификация может относиться к официальной личности или к абстрактным идентификаторам (псевдоним и т.д.). С помощью таких трекеров получается соотнести действия человека в онлайн и в аналоговом мире.	8
Отчет о сбоях и ошибках	Эти трекеры специализируются на сообщениях о сбоях приложений. Другими словами, их цель — уведомить разработчиков приложений о том, что приложение столкнулось с проблемой. Таким образом, информация, собранная в момент сбоя приложения, позволит разработчику исправить ошибку.	7
Обмен сообщениями и уведомления	Эти трекеры специализируются на мобильных push-уведомлениях и In-App Messaging, чтобы повысить уровень удержания и вовлеченности пользователей.	4
Чат	Этот трекер используется как готовое решение диалогового окна (чата) и помогает пользователю обращаться в службу поддержки или контактный центр, а также оставлять обратную связь.	1

Какие трекеры чаще всего установлены в приложениях

Большинство приложений (820 или 87,8%) имеет хотя бы один встроенный сторонний трекер.

Наиболее популярным трекером оказался Google Firebase Analytics¹⁹. Трекер установлен в 699 приложений (85,2%) и используется для анализа производительности мобильного приложения и оптимизации пользовательского опыта. Трекер собирает данные о поведении пользователей и позволяет измерить маркетинговые метрики. Ожидается, что трекер оказался самым популярным, так как он является бесплатным, а его установка в код мобильного приложения для Android — естественным решением в процессе разработки, поскольку трекер относится к экосистеме Google, создателя операционной системы Android.

¹⁹ <https://support.google.com/firebase/answer/7388022?hl=ru>

Вторым по популярности является трекер Google CrashLytics²⁰. Он установлен в 449 приложениях (54,8%) и используется для отслеживания сбоев и ошибок приложения, а также формирования о них отчетов для разработчика. По аналогии с трекером Google Firebase Analytics он является бесплатным и относится к экосистеме Google, возможна его интеграция в приложениях для Apple, Unity, Flutter.

Экосистема Google специально устроена таким образом, чтобы интегрировать большое число своих сервисов и инструментов разработки в создаваемые мобильные приложения. Это удобно для разработчиков, которые используют эти сервисы «из коробки», то есть без дополнительных усилий и платы.

Замыкает тройку наиболее популярных российский трекер AppMetrica²¹ от компании Яндекс, установленный в 407 приложениях (49,6%) – с почти двукратным опережением следующего места. Трекер собирает обезличенные данные о действиях пользователя в приложении для оптимизации маркетинговых кампаний. Фактически, трекер выступает аналогом аналитических трекеров от Google — является бесплатным аналитическим инструментом мобильных приложений, который активно используется на российском рынке маркетинга.

На российском рынке крупными технологическими гигантами, с собственной цифровой экосистемой многочисленных соцсетей, сервисов и мобильных приложений, являются компании Яндекс» и «VK». Подробнее о трекерах российских компаний смотрите в подразделе **«Приложения и трекеры компаний «Яндекс» и «VK»**.

В следующей таблице представлены трекеры, которые установлены в 100 приложениях и больше.

²⁰ <https://firebase.google.com/docs/crashlytics>

²¹ <https://appmetrica.yandex.ru/about>

Таблица 4. Какие трекеры чаще всего установлены в приложениях.

Трекер	Число приложений	Доля приложений	Страна	Компания	Категория
Google Firebase Analytics	699	74,8%	США	Google	Аналитика
Google CrashLytics	449	48,1%	США	Google	Отчет о сбоях и ошибках
AppMetrica	407	43,6%	Россия	Yandex	Аналитика
Google AdMob	234	25,1%	США	Google	Реклама
Facebook Login	172	18,4%	США	Meta	Идентификация
AppsFlyer	163	17,5%	США	AppsFlyer	Аналитика
Yandex Ad	163	17,5%	Россия	Yandex	Реклама
Facebook Analytics	147	15,7%	США	Meta	Аналитика
Facebook Share	145	15,5%	США	Meta	Аналитика
myTracker	144	15,4%	Россия	VK	Аналитика
IAB Open Measurement	133	14,2%	США	IAB Tech Lab	Реклама, идентификация
Huawei Mobile Services (HMS) Core	129	13,8%	Китай	Huawei	Реклама, аналитика, геолокация
Google Analytics	126	13,5%	США	Google	Аналитика
myTarget	120	12,8%	Россия	VK	Реклама
Vkontakte SDK (неофициальное)	115	12,3%	Россия	Peter Samokhin	Идентификация
Google Tag Manager	103	11%	США	Google	Аналитика

Категории приложений и число трекеров

Число трекеров, обнаруженных в приложениях, существенно отличается для разных категорий (мы использовали категории, определенные в магазине RuStore). Было подсчитано медианное число трекеров по всем приложениям в категории, в т.ч. учитывая приложения с нулевым значением трекеров. Данные представлены в таблице 5.

Антилидерами по медианному числу трекеров являются приложения категорий «Игры», «Новости», «Здоровье и спорт». При этом категория игр вторая по числу приложений вообще – в ней 152 приложения. И именно в ней встречается рекордное число трекеров в приложении – которое может достигать 37! Подробнее в в следующем **подразделе «Приложения с большим числом трекеров»**.

Категории «Государственные», «Финансы» и «Транспорт» можно назвать наиболее безопасными для пользователя: медианное число трекеров в них составляет всего 2-3. Хотя в некоторых случаях в них обнаруживаются и приложения с большим числом встроенных трекеров. Так, три образовательных приложения компании ООО «ЩИТ-В», посвященные сфере частной охранной деятельности, содержат по 21 трекеру, приложение «Экзамен ПДД 2022: билеты ГИБДД» имеет 15 трекеров, а финансовое приложение «КопиПросто - Простая копилка» — 12.

Особенное внимание мы обращаем на категорию «Государственные». Несмотря на то, что их меньше, чем в других категориях приложений (медианное значение составляет всего 2,5 трекера на приложение), в отличие от других приложений, государственные приложения являются безальтернативными. И должны максимально охранять пользователя от возможной утечки. Тем не менее, несмотря на борьбу самого государства с попаданием данных российских граждан в иностранные компании, среди обнаруженного в них кода трекеров встречаются в том числе и от компаний в зарубежных юрисдикциях – например:

- приложение Госуслуг (ru.rostel)²² включает трекеры от компании Google, такие как: Google CrashLytics, Google Firebase Analytics;
- приложение официальных штрафов ГИБДД (ru.gibdd_pay.app)²³ включает трекеры компаний Google (США), Adjust (Германия), Amplitude (США);

²² <https://apps.rustore.ru/app/ru.rostel>

²³ https://apps.rustore.ru/app/ru.gibdd_pay.app

- приложение Портал АСУЗ (ru.mosreg.easuz.portal)²⁴ включает трекеры компаний Google, Microsoft, MapBox.

Таких примеров много, почти все государственные приложения в России используют хотя бы один из сервисов компании Google, таких как Google CrashLytics и Google Firebase Analytics.

Таблица 5. Сколько трекеров установлено в приложение в зависимости от его категории.

Категория	Количество приложений	Медианное число трекеров на одно приложение в категории
Игры	152	9,3
Новости	38	9,1
Здоровье и спорт	55	7,5
Развлечения	120	5,9
Детские	3	5,0
Покупки	57	4,7
Объявления и услуги	43	4,7
Социальные	90	4,4
Образование	85	4,4
Медицина	29	4,3
Еда и напитки	32	4,2
Инструменты	192	3,7
Транспорт	83	3,5
Финансы	139	3,3
Государственные	45	2,5

²⁴ <https://apps.rustore.ru/app/ru.mosreg.easuz.portal>

Приложения с большим числом трекеров

В таблице 6 представлены 50 приложений с наибольшим числом установленных в них трекеров. По большей части они относятся к категориям «Игры» и «Развлечения».

Среди публикаторов самых нагруженных трекерами приложений “лидируют” HeroCraft (11), Lunapp (7), VK (7).

Таблица 6. Наиболее нагруженные трекерами приложения.

Название приложения	Название компании - публикатора приложения	Количество трекеров	Категория приложения из RuStore
Гильдия Героев: Экшен ММО РПГ	VK Play	37	Игры
Warface: GO	VK Play	36	Игры
Left to Survive	VK Play	34	Развлечения, Игры
Green button: Авто кликер игра	VK Play	28	Игры
Лови Конфету! Физический пазл	HeroCraft	28	Игры
Красный шарик: Возвращение!	HeroCraft	27	Игры
Juggernaut Wars - Raid Rpg	VK Play	27	Игры
Hoosegow: Prison Survival	D.Dream games	26	Игры, Развлечения
Shift Race: Гонки-трансформер	VK Play	26	Игры
Tank Battle: Танчики	BOLD CAT	25	Игры
Логика слов - игра на логику	Lunapp	25	Игры
Страны и Флаги: География мира	BOLD CAT	25	Игры
Улитка Боб: Пазл приключение	HeroCraft	24	Игры
Zausev.net: музыка для каждого	ООО "ЗАЙЦЕВ.НЕТ"	24	Развлечения
Мафиозо: Мафия - ПвП онлайн	HeroCraft	24	Игры, Развлечения

Лабиринт слов: найди слова	Lunapp	23	Игры
Небоскреб Мечты: Новые вершины	Overmobile	23	Игры
Shadow Fight Arena	Мобильные игры ООО	23	Игры
Карточные и настольные игры	Strict Games	23	Игры
Мистер Рыцарь : Пазл с булавами	HeroCraft	22	Игры
Голосовые заметки	ИП Мокрецов Роман Михайлович	22	Инструменты
Toy Car	Креос Дизайн	22	Игры
Datebox: знакомства и свидания	ИП Буйда Никита Юрьевич	22	Социальные
VOPP - вопросы для пар	ИП Буйда Никита Юрьевич	22	Социальные
Ферма "Веселые деньки"	HeroCraft	22	Игры
Филворды - темы	Lunapp	21	Игры
Слово за слово – игра в слова	ООО "Инкредибл мобайл энтертаймент"	21	Игры
GymUp - дневник тренировок	Iron Lab	21	Здоровье и спорт
Филворды - игра в поиск слов	Lunapp	21	Игры
Планета Самоцветов	Невософт	21	Игры
Законы и приказы для ЧО	ООО "ЩИТ-В"	21	Образование
Tempest: Море пиратов	HeroCraft	21	Игры
Кроссы - кроссворды на русском	Lunapp	21	Игры
World Above - Merge Puzzle	VK Play	21	Игры
Руководству ЧОО	ООО "ЩИТ-В"	21	Образование
Вход в СЭПО	ООО "ЩИТ-В"	21	Образование
Инструктаж ЧО	ООО "ЩИТ-В"	21	Образование
Red Ball 3: Красный шарик	HeroCraft	21	Игры
Space Arena: Собирай корабли	HeroCraft	20	Игры, Развлечения
Угадай слова	Lunapp	20	Игры
Тап Тап: Построй свой город	HeroCraft	20	Игры, Развлечения
Movika: Соцсеть коротких видео	ООО «Технологии интерактивного видео»	20	Развлечения, Социальные
Экзамен ПДД 2022: билеты ГИБДД	ООО «Реактив Фон»	20	Образование
Evo Puzzle - головоломки	Lunapp	20	Игры

КопиПросто - Простая копилка	Breakneck Apps	20	Финансы, Инструменты
Brawl King - Roguelike	HeroCraft	19	Игры
Небеса: Игры «три в ряд» с РПГ	ООО "ЭДРЕМ"	19	Игры
Предсказание по QR коду	ИП Горшенев Алексей Викторович	19	Развлечения, Игры
Кредитный калькулятор	ООО "СОКРАТ ПЛЮС"	19	Инструменты
101 HD	ИП Кулаков Андрей Сергеевич	18	Игры, Развлечения

Юрисдикции и компании

Каждый трекер является продуктом конкретной компании, то есть юридическому лицу, сервера, условия использования и политика приватности которого, привязаны к конкретной стране или территории местонахождения компании и/или центра обработки данных. В этом исследовании под юрисдикцией трекера принимается юрисдикция юридического лица, которое является владельцем сервиса и инфраструктуры трекера. В отличие от юрисдикций центров обработки данных оно чаще всего может быть гарантированно установлено и идентифицировано по его сайту, документам об условиях использования и общедоступным юридическим документам.

Как правило, юрисдикция совпадает со страной местонахождения штаб-квартиры, но могут встречаться и другие варианты, поэтому на практике юрисдикция должна быть указана явным образом в соглашении о конфиденциальности и условиях использования сервиса. Юрисдикция определяет то, законами какой страны/ территории руководствуется данная организация, в том числе в части требований местных правительств и специальных служб о доступе к данным. Так, на компании, зарегистрированные в Евросоюзе, распространяются требования GDPR, в России – закон о персональных данных в РФ, в США – зависит от штата и так далее. Например, трекеры в Швейцарии могут предоставлять данные только по решению суда, в то время как компании в США, Евросоюзе, России и других странах обязаны это делать в соответствии со своим законодательством, как правило, не требующим от специальных служб судебного решения. Мы исходим из того факта что правоохранительные органы и специальные служб стран в юрисдикции которых находятся компании владеющие продуктами трекеров обладают правовыми и иными возможностями для доступа к данным собираемых этими компаниями.

На уровне публичных деклараций BigTech-компании заявляют о намерениях противостоять запросам Правительств и сохранять конфиденциальность пользователей. К примеру, Google заявил, что будет удалять данные о местоположении пользователей после посещения ими клиник абортот и других мест, информация о которых относится к особо чувствительным и разглашение которой способно навредить человеку.²⁵ Это случилось после решения Верховного суда США, который постановил, что конституция США не предусматривает права на аборт на федеральном уровне.

В общем случае надо руководствоваться тем, что юридически правомерные запросы рассматриваются BigTech-компаниями. К примеру, известен случай, в котором с помощью ордера на обыск полиция штата Небраска (США) получила сведения из личных сообщений в Facebook и предъявила обвинение в совершении аборта.²⁶

Отслеживание пользователей через мобильные приложения (мобильный трекинг) — транснациональное явление. Оно заключается в высокой юридической и технической подвижности разработчиков мобильных приложений и сервисов для них. В частности, переключение между серверами от одной страны в другую может осуществляться за доли секунд, замена юрисдикции владельца сервиса немногим сложнее, но также может происходить без особых сложностей. При этом большое число сервисов выстраивают цепочки операторов данных, которые связаны между собой технологически и, относительно свободно, обмениваются информацией пользуясь тем, что не содержат данных, которые ранее считались персональными.

²⁵ <https://www.nytimes.com/2022/07/01/technology/google-abortion-location-data.html>

²⁶ <https://www.forbes.com/sites/emilybaker-white/2022/08/08/facebook-abortion-teen-dms/?sh=2da0325c579c>

Все это значительно усложняет не только работу регуляторов, но и приводит к невозможности пользователю знать всех операторов его данных и адекватно защитить свои права²⁷.

Что касается России, то на данный момент мобильные приложения, в том числе государственные, устроены таким образом, что содержат трекеры иностранных компаний, принадлежащих к юрисдикциям других стран. Это приводит к трансграничной передаче данных, собираемых о пользователях российских приложений.

Было обнаружено, что для приложений, имеющих как минимум один отслеживающий трекер, а таких 820 (87,8%), характерно следующее:

- Подавляющее большинство приложений (776 ед. или 94,6% от 820) имеют встроенные сторонние трекеры, принадлежащие юридическим лицам за пределами Российской Федерации.
- По числу приложений, к компаниям в зарубежных юрисдикциях которых принадлежат трекеры, лидируют: США, Россия и Китай. В 769 (93,8%) таких приложениях используются трекеры, принадлежащие компаниям юрисдикции США.
- 401 приложение (48,9%) имеет трекеры, принадлежащие как минимум 3 компаниям и больше.
- Российские трекеры, в основном принадлежащие компаниям «Яндекс» и «VK», используются в 477 (58%) приложениях. В большинстве случаев российские трекеры используются наряду с другими иностранными трекерами, выполняющими аналогичную и другие функции.
- Всего в 44 приложениях (5,3%) установлены только российские трекеры, без соседства с трекерами иных юрисдикций.

²⁷ <https://privacygsmobapps.infoculture.ru/>

Таблица 7. Статусы юрисдикций, трекары которых установлены в приложениях по отношению к России.

Юрисдикция	Число приложений	Статус страны	
		Признана недружественной Правительством РФ	Ввела санкции против России
США	769	Да	Да
Россия	477	-	-
Китай	151	Нет	Нет
Израиль	62	Нет	Нет
Канада	47	Да	Да
Великобритания	39	Да	Да
Япония	30	Да	Да
Германия	29	Да	Да
Франция	28	Да	Да
Индия	27	Нет	Нет
Чехия	3	Да	Да
Норвегия	2	Да	Да
Австрия	1	Да	Да
Турция	1	Нет	Нет
Швейцария	1	Нет	Да

Компании-авторы трекеров

Для тех приложений, что имеют хотя бы 1 установленный трекер, ожидаемо, лидируют трекеры компаний Big Tech:

- Google — 744 приложения (90,7%);
- Yandex — 407 приложений (49,6%);
- и Meta — 204 приложения (24,9%).

Таблица 8. Все компании, чьи трекеры установлены в более чем 100 приложениях.

Компания	В скольких приложениях установлен хотя бы один ее трекер	Доля приложений, %	Юрисдикция компании
Google	744	90,7%	США
Yandex	407	49,6%	Россия
Meta	204	24,9%	США
AppsFlyer	163	19,9%	США
VK	159	19,4%	Россия
IAB Tech Lab	133	16,2%	США
Huawei	129	15,7%	Китай
Peter Samokhin (разработчик неофициальной VKontakte SDK)	115	14 %	Россия

В 622 приложениях (75,8%) используются трекеры, которые связаны с 2-4 компаниями. А трекеры 15 и более компаний встречаются в 44 приложениях (5,4%). Большая часть таких приложений относится к категориям «Игры» и «Развлечения». Это говорит о том, что несмотря на формальную бесплатность представленных приложений, пользователь в реальности платит собственными данными, доступ к которым с помощью приложения получают многочисленные сторонние компании, владеющие установленными трекерами.

Таблица 9. Приложения с трекерами 15 и более различных компаний.

Приложение	Число компаний, которым принадлежат установленные в приложение трекеры	Число стран	Список стран	Категория приложения
Left to Survive	28	7	США, Россия, Израиль, Канада, Индия, Япония, Китай	Развлечения
Гильдия Героев: Экшен ММО РПГ	27	7	США, Россия, Израиль, Канада, Индия, Япония, Китай	Игры
Warface: GO	27	7	США, Россия, Израиль, Канада, Индия, Япония, Китай	Игры
Green button: Авто кликер игра	20	9	США, Россия, Израиль, Канада, Индия, Германия, Великобритания, Япония, Китай	Игры
Лови Конфету! Физический пазл	20	6	США, Россия, Канада, Индия, Япония, Китай	Игры
Shift Race: Гонки-трансформер	19	9	США, Россия, Израиль, Канада, Индия, Германия, Великобритания, Япония, Китай	Игры
Страны и Флаги: География мира	19	7	США, Россия, Израиль, Франция, Канада,	Игры

			Германия, Великобритания	
Мафиозо: Мафия - 18 ПвП онлайн	7		США, Россия, Канада, Индия, Великобритания, Япония, Китай	Игры
Красный шарик: 18 Возвращение!	6		США, Россия, Канада, Индия, Япония, Китай	Игры
VOPP - вопросы для пар	6		США, Китай, Россия, Израиль, Франция, Канада	Социальные
Datebox: знакомства и свидания	6		США, Китай, Россия, Израиль, Франция, Канада	Социальные
Законы и приказы для ЧО	6		США, Китай, Россия, Израиль, Франция, Канада	Образование
Juggernaut Wars - Raid Rpg	5		США, Израиль, Россия, Индия, Япония	Игры
Руководству ЧОО	6		США, Китай, Россия, Израиль, Франция, Канада	Образование
Zaycev.net: музыка для каждого	5		США, Россия, Израиль, Франция, Канада	Развлечения
Вход в СЭПО	6		США, Китай, Россия, Израиль, Франция, Канада	Образование
Hoosegow: Prison Survival	6		США, Россия, Израиль, Франция, Канада, Германия	Игры
Инструктаж ЧО	6		США, Китай, Россия, Израиль, Франция, Канада	Образование
Логика слов - игра на логику	5		США, Россия, Израиль, Франция, Канада	Игры
Мистер Рыцарь : Пазл с булавками	7		США, Россия, Израиль, Канада, Индия, Япония, Китай	Игры
Кроссы - кроссворды на русском	5		США, Россия, Израиль, Франция, Канада	Игры

Небоскреб Мечты: Новые вершины	17	6	США, Израиль, Россия, Канада, Индия, Япония	Игры
Tank Battle: Танчики	17	6	США, Россия, Израиль, Франция, Канада, Великобритания	Игры
Голосовые заметки	17	5	США, Россия, Израиль, Франция, Канада	Инструменты
World Above - Merge Puzzle	17	6	США, Израиль, Россия, Канада, Индия, Япония	Игры
Филворды - игра в поиск слов	17	5	США, Россия, Израиль, Франция, Канада	Игры
Филворды - темы	17	5	США, Россия, Израиль, Франция, Канада	Игры
Лабиринт слов: найди слова	16	5	США, Россия, Израиль, Франция, Канада	Игры
Предсказание по QR коду	16	5	США, Россия, Израиль, Франция, Канада	Развлечения
Evo Puzzle - головоломки	16	4	США, Россия, Израиль, Франция	Игры
Улитка Боб: Пазл приключение	16	7	США, Россия, Канада, Индия, Великобритания, Япония, Китай	Игры
GymUp - дневник тренировок	16	5	США, Россия, Израиль, Франция, Канада	Здоровье и спорт
Угадай слова	16	5	США, Россия, Израиль, Франция, Канада	Игры
Movika: Соцсеть коротких видео	16	7	США, Россия, Израиль, Канада, Индия, Япония, Китай	Развлечения
Планета Самоцветов	16	6	США, Россия, Израиль, Канада, Япония, Китай	Игры
Карточные и настольные игры	16	5	США, Россия, Израиль, Франция, Канада	Игры
Кредитный калькулятор	16	4	США, Россия, Израиль, Франция	Инструменты
Toy Car	16	6	США, Россия, Израиль, Канада, Индия, Япония	Игры
КопиПросто - Простая копилка	16	5	США, Россия, Израиль, Франция, Канада	Финансы

Red Ball 3: Красный шарик	16	5	США, Россия, Индия, Япония, Китай	Игры
Shadow Fight Arena	16	5	США, Израиль, Россия, Канада, Япония	Игры
Тап Тап: Построй свой город	15	5	США, Россия, Индия, Япония, Китай	Игры
Ферма "Веселые деньки"	15	5	США, Россия, Канада, Индия, Япония	Игры
Tempest: Море пиратов	15	5	США, Россия, Канада, Индия, Япония	Игры

Приложения и трекеры компаний «Яндекс» и VK28

Компании «Яндекс» и VK являются крупнейшими цифровыми экосистемами Рунета. По данным Mediascope совокупная аудитория многочисленных сервисов «Яндекса» и VK может достигать 65-80% от населения России.²⁹

Помимо разработки версий сервисов в вебе, компьютерных и мобильных приложений компании имеют собственные отслеживающие мобильные трекеры.

Таблица 10. Трекеры компаний «Яндекс» и VK.

Компания	Трекер	Число приложений	Доля, %
Яндекс	AppMetrica используется для измерения маркетинговых метрик и поведенческой аналитики пользователей.	407	49,6%
Яндекс	Yandex Ad30 помогает монетизировать приложения, размещать в приложениях рекламу и управлять ей.	163	19,8%

²⁸ Помимо трекеров компаний «Яндекс» и «VK» в списке трекеров был обнаружен российский неофициальный трекер «Vkontakte SDK» от независимого разработчика.

²⁹ <https://mediascope.net/data/>

³⁰ <https://yandex.ru/dev/mobile-ads/>

VK	myTracker — это пакет библиотек для сбора статистики по приложениям. ³¹ Собирает данные о действия пользователя, а также информацию об устройстве (идентификаторы, модель, ОС, версия, язык, размер экрана и пр.), информацию о сети (оператор, тип соединения, WiFi, Bluetooth), местоположение устройства (только с согласия пользователя и если соответствующий запрос встроен в приложение).	144	17,6%
VK	myTarget ³² — трекер, предназначенный для настройки целевой рекламы. Отслеживает пользователей социальных сетей ВКонтакте и Одноклассники. По device/ advertising ID, который отправляется в myTarget, идентифицируется за пользователь и определяется релевантная для него реклама.	120	14,6%
VK	Mail.ru — библиотека, предназначенная для облегчения авторизации в Mail.ru. ³³	11	1,3%

Имея набор данных о трекерах и приложениях, разработанных компаниями «Яндекс» и «VK», изучим какие трекеры преобладают в их сервисах (смотреть Диаграммы 3 и 4).

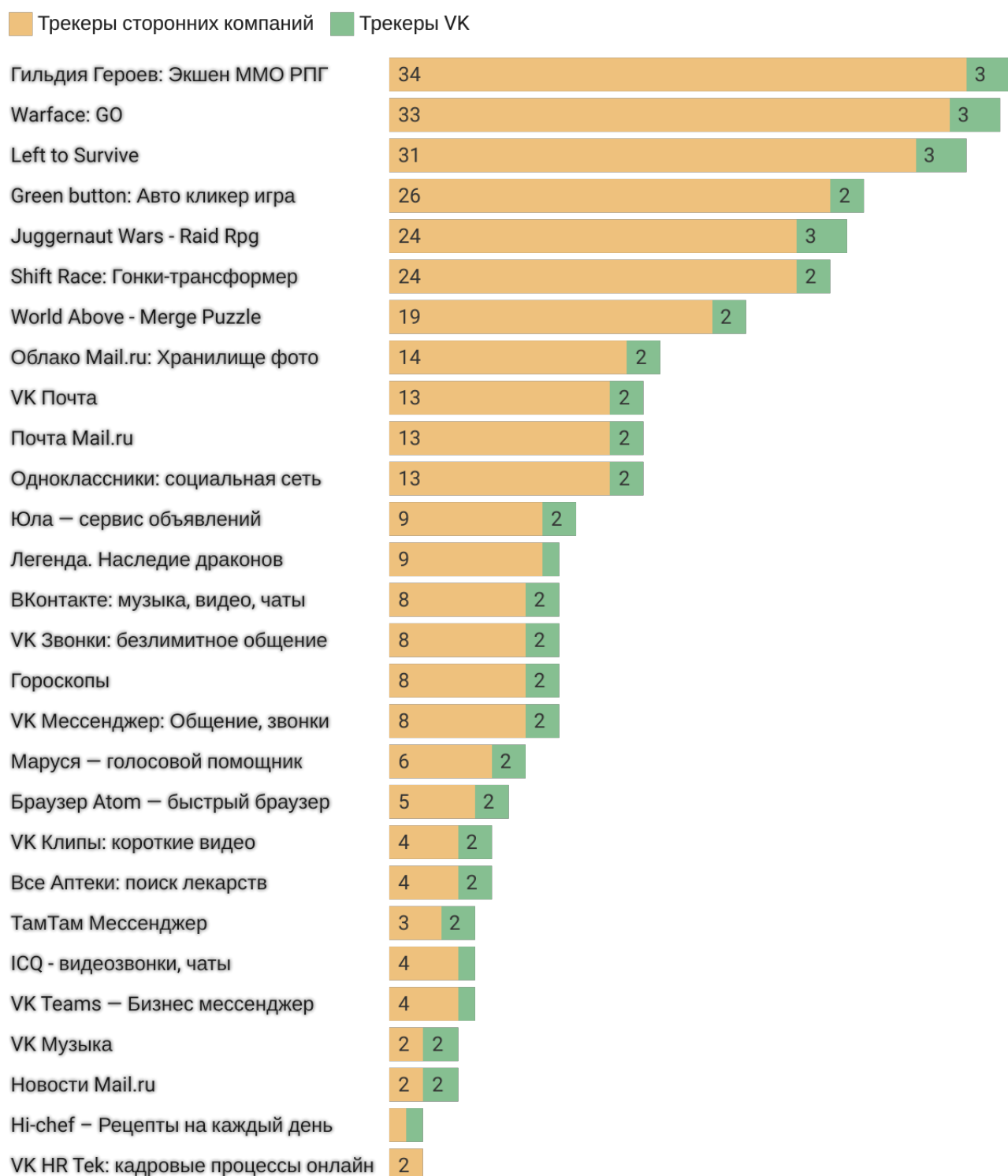
³¹ <https://tracker.my.com/docs/sdk/about?lang=ru>

³² <https://target.my.com/help/partners/mob/faq/ru>

³³ <https://o2.mail.ru/docs#android>

Трекеры в приложениях VK

В подсчет включены трекеры приложений, опубликованные VK Play.



Created with Datawrapper

Диаграмма 3. Трекеры в приложениях VK

Игровые приложения, изданные VK, являются наиболее нагруженными по числу трекеров. Из 28 приложений в 17 установлено 10 и более трекеров, достигая значения 34. К примеру, приложения с 30 и большим числом трекеров: «Гильдия героев: Экшен ММО РПГ», «Warface: GO», «Left to Survive».

Помимо этого, значительно преобладают трекеры, созданные сторонними компаниями, и нет ни одного приложения, в котором были бы установлены только трекеры VK.

Трекеры в приложениях Яндекса



Created with Datawrapper

Диаграмма 4. Трекеры в приложениях Яндекс

По сравнению с VK, в опубликованных в магазине RuStore приложениях «Яндекса», используется не так много трекеров и значительно меньше используются трекеры сторонних компаний. Наиболее нагруженными трекерами приложениями являются:

- Яндекс.Маркет — 10 трекеров, 9 из которых сторонние.
- Яндекс Go: такси и доставка — 6 трекеров, 5 из которых сторонние.

Также среди 10 приложений «Яндекса» есть 3 приложения, в которые нет ни одного трекера сторонней компании, но установлена AppMetrica. Это приложения «Яндекс Переводчик», «Яндекс Клавиатура», «Яндекс Разговор: помощь глухим».

Таблица 11. Трекеры в приложениях VK

Приложение	Трекеры российских компаний	Трекеры иностранных юрисдикций	Общее число трекеров	Число трекеров иностранных юрисдикций	Юрисдикции трекеров
Гильдия Героев: Экшен MMO РПГ	Yandex Ad, AppMetrica, myTracker, myTarget, Mail.ru, VKontakte SDK	AppsFlyer, Flurry, Google CrashLytics, Ogury Presage, Twitter MoPub, Google Analytics, Google Firebase Analytics, ChartBoost, Facebook Ads, Facebook Analytics, Facebook Login, Facebook Share, AppLovin (MAX and SparkLabs), Smaato, AdColony, Amazon Advertisement, Fyber, Inmobi, Unity3d Ads, ironSource, Vungle, PubNative, HyprMX, Tapjoy, Mintegral, Google AdMob, Verizon Ads, maio by i-mobile, IAB Open Measurement, Mail.ru, Pangle, Snap Ad Kit	37	31	США, Индия, Россия, Израиль, Япония, Китай, Канада
Warface: GO	Yandex Ad, AppMetrica, myTracker, myTarget, Mail.ru, VKontakte SDK	AppsFlyer, Flurry, Google CrashLytics, Ogury Presage, Twitter MoPub, Google Firebase Analytics, ChartBoost, Facebook Ads, Facebook Analytics, Facebook Login, Facebook Share, AppLovin (MAX and SparkLabs), Smaato, AdColony, Amazon Advertisement, Fyber, Inmobi, Unity3d Ads, ironSource, Vungle,	36	30	США, Индия, Россия, Израиль, Япония, Китай, Канада

		PubNative, HyprMX, Tapjoy, Mintegral, Google AdMob, Verizon Ads, maio by i-mobile, IAB Open Measurement, Pangle, Snap Ad Kit			
Left to Survive	Yandex Ad, AppMetrica, myTracker, myTarget, Mail.ru, VKontakte SDK	AppsFlyer, Flurry, Google CrashLytics, Ogury Presage, Twitter MoPub, Google Firebase Analytics, ChartBoost, Moat, Facebook Ads, AppLovin (MAX and SparkLabs), Smaato, AdColony, Amazon Advertisement, Fyber, Inmobi, Unity3d Ads, ironSource, Vungle, PubNative, HyprMX, Tapjoy, Mintegral, Google AdMob, Verizon Ads, maio by i-mobile, IAB Open Measurement, Pangle, Snap Ad Kit	34	28	США, Индия, Россия, Израиль, Япония, Китай, Канада
Green button: Авто кликер игра	Yandex Ad, AppMetrica, myTracker, myTarget	Google CrashLytics, Ogury Presage, Google Firebase Analytics, Adjust, Facebook Ads, Facebook Analytics, Facebook Login, Facebook Share, AppLovin (MAX and SparkLabs), AdColony, Amazon Advertisement, Fyber, Inmobi, Unity3d Ads, ironSource, Vungle, PubNative, HyprMX, Tapjoy, Mintegral, GameAnalytics, Google AdMob, IAB Open Measurement, Pangle	28	24	США, Германия, Индия, Россия, Израиль, Япония, Китай, Великобритания, Канада
Juggernaut Wars - Raid Rpg	myTracker, myTarget, Mail.ru, VKontakte SDK	AppsFlyer, Flurry, HockeyApp, Google Analytics, Google Firebase Analytics, ChartBoost, Moat, Facebook Ads, Facebook Analytics, Facebook Login, AppLovin (MAX and SparkLabs), AdColony, Fyber, Google Tag Manager, Inmobi, Unity3d Ads, ironSource, Vungle, HyprMX, Tapjoy, Microsoft Visual Studio App Center Crashes, Google AdMob, IAB Open Measurement	27	23	США, Германия, Индия, Израиль, Россия, Япония

Shift Race: Гонки- трансформер	AppMetrica, myTracker, myTarget,	Google CrashLytics, Ogury Presage, Google Firebase Analytics, Adjust, Facebook Ads, Facebook Analytics, Facebook Login, Facebook Share, AppLovin (MAX and SparkLabs), AdColony, Amazon Advertisement, Fyber, Inmobi, Unity3d Ads, ironSource, Vungle, HyprMX, Tapjoy, Mintegral, GameAnalytics, Google AdMob, IAB Open Measurement, Pangle	26	23	США, Германия, Индия, Россия, Израиль, Япония, Китай, Великобрита ния, Канада
World Above - Merge Puzzle	myTracker, Mail.ru, VKontakte SDK	AppsFlyer, Google Firebase Analytics, ChartBoost, Moat, Facebook Ads, Facebook Analytics, Facebook Login, AppLovin (MAX and SparkLabs), Fyber, Inmobi, Unity3d Ads, ironSource, Vungle, Tapjoy, Microsoft Visual Studio App Center Crashes, Google AdMob, IAB Open Measurement, Pangle	21	18	США, Индия, Израиль, Россия, Япония, Канада
Облако Mail.ru: Хранилище фото	myTracker, myTarget, VKontakte SDK	AppsFlyer, Schibsted, Google Firebase Analytics, Facebook Analytics, Facebook Login, Facebook Share, Unity3d Ads, ironSource, Microsoft Visual Studio App Center Crashes, Microsoft Visual Studio App Center Analytics, Google AdMob, IAB Open Measurement, Huawei Mobile Services (HMS) Core	16	13	США, Норвегия, Израиль, Россия, Китай
VK Почта	myTracker, myTarget, VKontakte SDK	AppsFlyer, Flurry, Google CrashLytics, Google Analytics, Google Firebase Analytics, Facebook Ads, Google Tag Manager, Microsoft Visual Studio App Center Crashes, Microsoft Visual Studio App Center Analytics, Google AdMob, IAB Open Measurement, Huawei Mobile Services (HMS) Core	15	12	США, Россия, Китай
Почта Mail.ru	myTracker, myTarget, VKontakte SDK	AppsFlyer, Flurry, Google CrashLytics, Google Analytics, Google Firebase Analytics, Facebook Ads, Google Tag Manager, Microsoft Visual	15	12	США, Россия, Китай

		Studio App Center Crashes, Microsoft Visual Studio App Center Analytics, Google AdMob, IAB Open Measurement, Huawei Mobile Services (HMS) Core			
Одноклассник и: социальная сеть	myTracker, myTarget, VKontakte SDK	AppsFlyer, Google CrashLytics, Google Analytics, Google Firebase Analytics, Facebook Ads, Facebook Analytics, Facebook Login, Facebook Share, Google Tag Manager, ironSource, Google AdMob, IAB Open Measurement	15	12	США, Израиль, Россия
Юла — сервис объявлений	myTracker, myTarget, VKontakte SDK	AppsFlyer, Google CrashLytics, Google Analytics, Unity3d Ads, ironSource, Google AdMob, IAB Open Measurement, Huawei Mobile Services (HMS) Core	11	8	США, Израиль, Россия, Китай
Легенда. Наследие драконов	myTracker, VKontakte SDK	Google Analytics, Moat, AppLovin (MAX and SparkLabs), AdColony, Unity3d Ads, ironSource, Vungle, IAB Open Measurement	10	8	США, Израиль, Россия
ВКонтакте: музыка, видео, чаты	myTracker, myTarget, VKontakte SDK	AppsFlyer, Google CrashLytics, Google Analytics, Facebook Analytics, Facebook Login, Facebook Share, IAB Open Measurement	10	7	США, Россия
VK Звонки: безлимитное общение	myTracker, myTarget, VKontakte SDK	AppsFlyer, Google CrashLytics, Google Analytics, Facebook Analytics, Facebook Login, Facebook Share, IAB Open Measurement	10	7	США, Россия
Гороскопы	myTracker, myTarget	Flurry, Google CrashLytics, Google Analytics, Facebook Ads, Facebook Analytics, Facebook Login, Facebook Places, Facebook Share	10	8	США, Россия
VK Мессенджер: Общение, звонки	myTracker, myTarget, VKontakte SDK	AppsFlyer, Google CrashLytics, Google Analytics, Facebook Analytics, Facebook Login,	10	7	США, Россия

		Facebook Share, IAB Open Measurement			
Маруся — голосовой помощник	myTracker, myTarget, VKontakte SDK	Google CrashLytics, Google Firebase Analytics, Microsoft Visual Studio App Center Crashes, IAB Open Measurement, Huawei Mobile Services (HMS) Core	8	5	США, Россия, Китай
Браузер Atom — быстрый браузер	myTracker, myTarget, VKontakte SDK	AppsFlyer, Google CrashLytics, Google Firebase Analytics, Google AdMob	7	4	США, Россия
VK Клипы: короткие видео	myTracker, myTarget, VKontakte SDK	Google CrashLytics, Google Firebase Analytics, IAB Open Measurement	6	3	США, Россия
Все Аптеки: поиск лекарств	myTracker, myTarget, VKontakte SDK	AppsFlyer, Google CrashLytics, Google Firebase Analytics	6	3	США, Россия
ТамТам Мессенджер	myTracker, myTarget, VKontakte SDK	Google CrashLytics, Google Firebase Analytics	5	2	США, Россия
ICQ - видеозвонки, чаты	myTracker	HockeyApp, Google Firebase Analytics, Microsoft Visual Studio App Center Crashes, Microsoft Visual Studio App Center Analytics	5	4	США, Германия, Россия
VK Teams — Бизнес мессенджер	myTracker	HockeyApp, Google Firebase Analytics, Microsoft Visual Studio App Center Crashes, Microsoft Visual Studio App Center Analytics	5	4	США, Германия, Россия
VK Музыка	myTracker, myTarget, VKontakte SDK	AppsFlyer	4	1	США, Россия
Новости Mail.ru	myTracker, myTarget	Google CrashLytics, Google Firebase Analytics	4	2	США, Россия
Hi-chef – Рецепты на каждый день	myTracker	Google Firebase Analytics	2	1	США, Россия
VK HR Tek: кадровые процессы онлайн	-	Google CrashLytics, Google Firebase Analytics	2	2	США

Таблица 12. Трекеры в приложениях компании «Яндекс».

Приложение	Трекеры российских компаний	Трекеры иностранных юрисдикций	Общее число трекеров	Число трекеров иностранных юрисдикций	Юрисдикции трекеров
Яндекс.Маркет: здесь покупают	AppMetrica, VKontakte SDK	Google CrashLytics, Google Analytics, Google Firebase Analytics, Adjust, Facebook Login, Facebook Share, Google Tag Manager, Huawei Mobile Services (HMS) Core	10	8	США, Германия, Россия, Китай
Яндекс Go: такси и доставка	AppMetrica	Google Analytics, Google Firebase Analytics, Adjust, Google Tag Manager, Huawei Mobile Services (HMS) Core	6	5	США, Германия, Россия, Китай
Яндекс.Браузер — с Алисой	Yandex Ad, AppMetrica	Facebook Login, Facebook Share, Huawei Mobile Services (HMS) Core	5	3	США, Россия, Китай
Яндекс — с Алисой	Yandex Ad, AppMetrica	Facebook Login, Facebook Share, Huawei Mobile Services (HMS) Core	5	3	США, Россия, Китай
Яндекс Навигатор	Yandex Ad, AppMetrica	Google CrashLytics, Google Firebase Analytics	4	2	США, Россия
Яндекс Карты и Навигатор	AppMetrica	Google CrashLytics, Schibsted, Huawei Mobile Services (HMS) Core.	4	3	США, Норвегия, Россия, Китай
Яндекс Метро	Yandex Ad, AppMetrica	Google CrashLytics	3	1	США, Россия
Яндекс Переводчик	AppMetrica	-	1	0	Россия
Яндекс Клавиатура	AppMetrica	-	1	0	Россия
Яндекс Разговор: помощь глухим	AppMetrica	-	1	0	Россия

Разрешения

Разрешения (permissions) — это права, которые получает мобильное приложение на устройстве для доступа к тем или иным его функциям. Разрешения могут быть неопасными, не связанными с доступом к личными данным, например, использование интернета, а могут нести потенциальную угрозу слежки или злонамеренного использования, например доступ к точным координатам или же к камере и микрофону устройства.

К потенциально опасным разрешениям относятся разрешения, которые могут повлиять на конфиденциальность пользователя или работу устройства в соответствии с уровнем защиты Android от Google (для Android 10, уровень API 29³⁴ и выше). Уровень защиты — это общий порядок использования разрешений, описание различных типов разрешений и некоторые лучшие практики использования разрешений в приложении.

Пользователь должен в явно выраженном виде дать согласие на предоставление доступа этим разрешениям. К ним относятся доступы к камере, контактам, календарю, данным о приблизительном или точном местоположении, микрофону, датчикам, хранилищу, совершению звонков, отправке SMS и другим.

Функциональность некоторых приложений зависит от доступа к конфиденциальной информации пользователя, связанной с журналами вызовов, хранилищем и SMS-сообщениями. Такие разрешения необходимы для работы приложения, то есть использование

³⁴ <https://developer.android.com/guide/topics/permissions/overview>

потенциально опасных разрешений не обязательно негативно влияет на конфиденциальность данных пользователя.

Однако приложения могут запрашивать и собирать избыточное количество данных, что закономерно вызывает вопросы. Например, если при отсутствии понятных пользователю функций работы с изображением с камеры приложение просит доступа к камере – повод насторожиться. При этом у пользователя существует контроль над этими разрешениями. В зависимости от смартфона можно ограничить некоторые из этих разрешений, зайдя в настройки телефона.

Не всегда функционал, для которого нужно разрешение, лежит на поверхности. Так, в банковских приложениях («Сбербанк Онлайн», «ВТБ Онлайн» и др.) является обычной практикой запрашивать доступ к камере устройства. Это объясняется необходимостью фотографировать QR-коды или карточки для распознавания номера, иногда – для распознавания клиента по лицу.

Аналогично с доступом к данным о местоположении устройства. Без доступа к этим данными приложения карт, такси, каршеринга, доставки не смогут полноценно и корректно работать, а приложение банка не подскажет вам ближайший банкомат.

В качестве контрпримера: приложение «Метро Москвы» запрашивает разрешение на совершение телефонных вызовов. Не совсем понятно для реализации какого пользовательского сценария разработчики включили это разрешение.

Помимо очевидного несоответствия между ожидаемой функциональностью приложения и набором запрашиваемых разрешений есть другой способ обнаружения потенциально проблемных мест. Если выборочно сравнить набор разрешений схожих по смыслу и функциям приложений, то становится ясно, что у одного из приложений может быть

таких разрешений избыточное число. Например, приложение онлайн-кинотеатра «Wink – ТВ, фильмы, сериалы» (разработчик — ПАО «Ростелеком») запрашивает доступ к точному местоположению пользователя и записи аудио, тогда как аналогичные приложения — только чтение и запись в хранилище данных, что объясняется необходимостью сохранять и кэшировать³⁵ данные мультимедиа.

Сколько разрешений (в том числе потенциально опасных) требуется, должно зависеть от каждого конкретного случая его применения. В среде разработки мобильных приложений встречается сценарий, при котором организация, владеющая продуктом, передает разработку приложения на субподряд сторонней компании. Как правило, субподрядчик имеет готовый шаблон приложения, который он использует повторно для каждого нового приложения. В таком случае все разрабатываемые приложения будут включать эти разрешения, независимо от того, указаны они в техническом задании или нет.

Среди 934 исследованных приложений было обнаружено 602 уникальных разрешения, из которых 19 относятся к потенциально опасным, согласно списку уровней защиты для Android от Google³⁶.

- Большинство приложений (821 единица или 88%) запрашивает как минимум одно потенциально опасное разрешение.
- Только в 176 (18,8%) приложениях не обнаружено потенциально опасных разрешений.
- Всего в 17 приложениях (1,8%) нет запроса ни одного разрешения доступа к функциям и данным устройства, а также нет ни одного установленного трекера.

³⁵ Высокоскоростной уровень хранения данных временного характера:

<https://aws.amazon.com/ru/caching/>

³⁶ <https://developer.android.com/guide/topics/permissions/overview>

- Из потенциально опасных разрешений в приложениях чаще всего встречаются: доступ на чтение и запись во внешнее хранилище данных, доступ к камере, доступ к точному и приблизительному местоположению, получению информации об устройстве и записи аудио.
- Из 29 приложений, в которых установлено 10 и более опасных разрешений (Таблица 14), более трети (10) принадлежат одному разработчику — компании VK.
- Больше всего таких разрешений запрашивают приложения «VK Звонки: безлимитное общение» (14), «Одноклассники: социальная сеть» (14), «ICQ - видеозвонки, чаты» (13), которые принадлежат компании VK.

Таблица 13. Список опасных разрешений и число приложений, в которых они установлены.³⁷

Разрешение	Число приложений	Доля приложений, %
Запись во внешнее ³⁸ хранилище данных — приложение-владелец может получить доступ к внешнему хранилищу и коллекциям визуальных и аудио медиафайлов	691	74%
Чтение внешнего хранилища данных — позволяет приложению изменять и удалять медиафайлы на данном устройстве или любом подключенном устройстве хранения без подтверждения пользователя	515	55,1%
Доступ к камере и ко всем ее функциям	425	45,5%
Доступ к точному местоположению	374	40%
Доступ к приблизительному местоположению	343	36,7%
Чтение информации об устройстве — получает доступ к сведениям о состоянии телефона, включая текущую информацию о сотовой сети,	207	22,2%

³⁷ <https://developer.android.com/reference/android/Manifest.permission>

³⁸ <https://www.digitalocean.com/community/tutorials/android-external-storage-read-write-save-file>

статус всех текущих вызовов и список всех Phone Accounts, зарегистрированных на устройстве		
Доступ к записи аудио позволяет приложению записывать звук	201	21,5%
Получение информации об аккаунтах позволяет получить доступ к списку учетных записей в службе Accounts Service	111	11,9%
Чтение контактов позволяет приложению читать данные контактов пользователя	113	12,1%
Совершение звонка позволяет приложению инициировать телефонный вызов без прохождения через пользовательский интерфейс Dialer для подтверждения пользователем	74	7,9%
Запись данных из календаря позволяет приложению записывать данные календаря пользователя	59	6,3%
Чтение календаря позволяет приложению считывать данные календаря пользователя	58	6,2%
Запись контактов позволяет приложению записывать данные контактов пользователя	30	3,2%
Чтение телефонного номера позволяет получить доступ на чтение к телефонному номеру (номерам) устройства	22	2,4%
Чтение журнала телефонных вызовов пользователя	11	1,2%
Доступ к принятию вызова позволяет приложению отвечать на входящий телефонный звонок	4	0,4%
Позволяет приложению использовать службу SIP (Session Initiation Protocol — протокол установления сеанса) — один из протоколов, который обеспечивает обмен данными в сети в формате мультимедиа	3	0,3%
Доступ к датчикам тела позволяет приложению получить доступ к данным с датчиков, которые пользователь использует для измерения происходящего внутри своего тела, например, частоты сердечных сокращений	2	0,2%
Получение SMS-сообщений приложением	1	0,1%

Таблица 14. Приложения, в которых установлено 10 и более опасных разрешений.

Приложение	Число опасных разрешений
VK Звонки: безлимитное общение	14
Одноклассники: социальная сеть	14
ICQ - видеозвонки, чаты	13
ВТБ Онлайн	13
Маруся — голосовой помощник	12
VK Мессенджер: Общение, звонки	12
ВКонтакте: музыка, видео, чаты	12
VK Teams — Бизнес мессенджер	12
Тинькофф Джуниор	11
VK Клипы: короткие видео	11
NG Academy	11
ТамТам Мессенджер	11
Юла — сервис объявлений	11
Тинькофф Мобильный банк	11
Яндекс Навигатор	11
Кредит онлайн: кредитная карта	10
SkolCity "Сколково"	10
СГБ МОБАЙЛ	10
СберБанк Онлайн – с Салютом	10
Альфа-Банк	10
Яндекс Карты и Навигатор	10
1F Mobile	10
Диалог регионы	10
Яндекс Go: такси и доставка	10
ВкусВилл for Staff	10
Северсталь. Учись мобильно	10
Тинькофф Мобайл: сотовая связь	10
Тинькофф Бизнес для ИП и ООО	10
GEOZON Care	10

Рекомендации

1. Регуляторам — сформировать стандарт соблюдения приватности для мобильных приложений, разрабатываемых за счёт средств федерального бюджета и бюджетов субъектов федерации, а также естественных монополий в рамках контрактных работ по 44-ФЗ, 223-ФЗ и, например, бюджетными учреждениями при выполнении государственных заданий.
2. Магазинам приложений — разработать для публикаторов правила по обязательному раскрытию информации о наличии специальных разрешений, сборе данных в мобильных приложениях и их передаче сторонним лицам по аналогии со стандартом Data Safety у Google Play.
3. Заказчикам разработки приложений — включать требования по соблюдению приватности в техническое задание по созданию и разработке приложения, а также проводить регулярный аудит ранее разработанных приложений на соблюдение базовых требований приватности, в том числе, по критериям отсутствия кода трекеров, передающих сведения без обязательного обоснования.
4. Осуществлять регулярный контроль за соблюдением разработанных требований к приватности мобильных приложений.
5. Всем участникам рынка создать и поддерживать каналы обратной связи для коммуникации с гражданами и организациями по вопросам, предложениям и жалобам о фактах несоблюдения приватности.
6. Выстраивать практику саморегулирования рынка мобильных приложений, например, в виде соответствующей хартии и создания стандартов раскрытия информации совместно с некоммерческими организациями, регуляторами и иными организациями, действующими в защиту интересов граждан и потребителей.

7. Организовывать регулярные исследования рынка, цель которых изучить — методы сбора и обработки данных о пользователях в экосистемах мобильных платформ, таких как Android, и актуализация обязательных требований и методических рекомендаций по раскрытию информации.