Вычислительная свобода на мобильном устройстве

Облегченное практическое пособие

Пособие создано в рамках проекта LibreTrack

Вычислительная свобода на мобильном устройстве. Облегченное практическое пособие

В пособии разъяснены принципы работы мобильных сетей и устройств. Рассмотрены угрозы, связанные с ними. Приведены практические инструкции по безопасной настройке мобильных устройств, а также использованию различных свободных приложений и сетевых сервисов.

Папка с материалами проекта LibreTrack в сервисе Internxt https://share.internxt.com/d/sh/folder/bb248f9bfd080972c8f1/765d77934c48a5857b51e6a2972bc41ae02147b25e53e07878471ae8539077d3

Канал YouTube https://www.youtube.com/channel/UCDhg72ALuEhO0BkkyWHt2JA

Оглавление

1 Предисловие

Данное пособие является вырезкой материалов по настройке безопасной системы на мобильном устройстве из полного пособия по вычислительной свободе.[1] Из него удалено множество материалов, которые для обычного пользователя являются явно избыточными. Материалы, требовавшие обновления, актуализированы. Также внесены сведения, которые прежде не входили в полное пособие, но которые также представляются важными для пользователей смартфонов и планшетов.

Эти инструкции рассчитаны на пользователей не искушенных в компьютерных технологиях, изложение дается достаточно ясно.

2 Сведения о мобильных сетях и устройствах

1 Принципы работы сотовой сети

При использовании мобильного устройства принципы информационной безопасности необходимо соблюдать также, как и при использовании компьютера. Для мобильников, при этом, характерны свои особые риски, связанные с особенностью их устройства и функций. Для того, чтобы их осветить, необходимо объяснить, как функционируют мобильные телефоны в сотовой сети. Это важно для понимания не только того, как осуществляется сотовая связь, но и каким образом определяется местоположение телефонов.

Вышки сотовой связи — базовые станции — непрерывно излучают радиоволновые сигналы на определенных частотах. Мобильный телефон эти сигналы принимает, определяет какая конкретно базовая станция их послала (эта информация закодирована в сигнале), определяет силу этого сигнала, и на основании этой самой силы сигнала, выбирает ту базовую станцию, от которой этот сигнал сильнее всего. К выбранной станции он сам уже отсылает сигнал о том, что находится в зоне ее действия. Сигнал от базовой станции распространяется на определенное расстояние, образуя вокруг нее как бы «соту», в пределах которой он действует. Соответственно, вся сеть состоит из таких вот, перекрывающих друг дружку «сот».[2]

Если базовая станция отсылает сигналы непрерывно, то телефон большую часть времени находится в режиме пассивного приема, сам ничего не посылая. Отсылает он сигнал в следующих случаях. При включении и выключении. При

перемещении, когда телефон чувствует, что сигнал от одной вышки, в зоне действия которой он был до сих пор, ослаб, а от другой усилился, он переключается между ними, посылая сигнал, соответственно, той, сигнал которой стал сильнее. При совершении звонка, отправке SMS и т.п. Через определенные периоды времени, находясь в простое, обычно, раз в час. Таким образом, сеть всегда знает, где находится телефон, если он включен — в зоне действия какой станции. И когда совершается звонок или отправляется SMS на определенный номер, сеть отправляет сигнал на ту вышку, в зоне действия которой, последний раз обнаруживал себя нужный телефон. И она уже распространяет сигнал о вызове, в котором закодировано, для какого номера он предназначен, после чего соответствующий телефон, приняв его, уведомляет о звонке.[1]

Вот так вкратце работает сотовая сеть. Конечно, это невероятно схематично и упрощенно. Но этого вполне достаточно для принципиального понимания работы мобильной сети, а также того, как можно отследить телефон, находящийся в этой сети.

2 Определение местоположения телефона

Поскольку сети известно, в районе действия какой базовой станции, находится телефон, если известны координаты этой станции, его можно отследить с точностью до нее. Вернее, с точностью до того радиуса, на который распространяется сигнал от этой базовой станции. В случае обычной соты, радиус составляет около 30 км, в некоторых случаях до 70, а то и до 120 км.[2] Понятное дело, что если вас отследят с такой точностью, считайте, что вас не отследили вообще. В обычной сельской местности, достаточно заселенной, в маленьких городах и пригородах, также действуют микросоты, и точность может составлять от 1 до 5 км.[3] В крупных городах, где также стоят малые соты, в том числе, пикосоты, точность может составлять от 100 до 500 м.[4] А в случае фемтосоты, до 10 м.[5] Последние очень редки, и в случае их, вряд ли есть необходимость делать уточнения. А вот в остальных случаях, вопрос об увеличении точности, ставить вполне правомерно.

Существует специальное оборудование, позволяющее измерять время прохождения сигнала от станции до мобильника и обратно. В случае применения такого оборудования, точность может значительно возрасти. К примеру, если без него точность составляет несколько километров, то с ним,

она уже будет составлять несколько сотен метров.[6] Но у этого способа есть свои минусы, которые в некоторых случаях сводят его преимущества на нет. Данный способ не может учесть, во-первых, затухание сигнала. Во-вторых, отражение сигнала. Если вы находитесь посреди зданий, то сигнал дойдет до вышки многократно отражаясь, и соответственно, придет не из того места, где находитесь вы.[7] Такой способ может повысить точность в разряженной местности, например, где-то в сельской округе. А в плотно застроенном городе, наоборот, снизит ее. Возможно, некоторые слышали о компаниях, которые продают операторам мобильной связи оборудование, позволяющее отслеживать мобильные телефоны с точностью до одного метра. Это то самое оборудование, о котором я сейчас говорил. Откуда же такая точность? Это стандартный маркетинговый ход. Указывается лучший результат испытаний, проведенных в самых благоприятных условиях. В пустынной местности, если телефон недалеко от вышки, точность может быть очень высокой. Тем более, если это фемтосота, то отследить с точностью до одного метра вполне можно. На практике же, даже в крупном городе, где высокая плотность вышек, вряд ли удастся достичь точности больше, чем сотня-другая метров.

Также наверняка многие слышали о такой вещи, как триангуляция. Якобы, оператор смотрит, в зоне действия каких вышек находится телефон, какова сила сигнала от этого телефона на каждой вышке, и по интегральной картине от силы сигнала на нескольких вышках, определяет местоположение телефона с большой точностью. Теоретически такое возможно, но чтобы осуществить это на практике необходимо серьезно модифицировать сотовую сеть в целом. Кроме того, остается все та же проблема, что и с измерением времени прохождения сигнала, нельзя учесть затухание сигнала и его отражение. Поэтому даже в случае осуществления триангуляции результат может оказаться весьма сомнительным, и явно не будет стоить тех затрат, которые были сделаны для его получения.[8]

Однако телефон, постоянно принимая сигналы от нескольких станций и измеряя их силу, может провести эту самую триангуляцию. То есть сам телефон способен таким образом сам определить свое примерное местоположение. Однако, для его определения ему не хватает информации, собственно, о координатах базовых станций, с которых он получает сигнал.[9]

Такие приложения для поиска телефона, как Google Latitude, которые определяют местонахождение даже без GPS, скорее всего, знают координаты

вышек, от тех пользователей той же программы, у которых GPS есть. То есть, телефоны тех пользователей, у кого на них включен GPS, анализируют сигналы от вышек сотовой сети и передают в компанию, контролирующую это приложение, данные о том, в каком регионе, какие вышки действуют. То же приложение, установленное у других пользователей, пользуясь базами данных, разработавшей ее компании, получает информацию об этих вышках и может уже, ориентируясь по ним, примерно определять местонахождение мобильника без GPS. Кстати, при таком способе, точность также не превышает ста метров. [10]

Для того, чтобы лучше представлять, как происходит отслеживание телефона по вышкам сотовой связи, полезно знать какую информацию телефон им отсылает. Во-первых, это конечно, номер телефона. Во-вторых, IMSI — уникальный идентификатор абонента.[11] А в случае повторной связи с вышкой TMSI — временный идентификатор абонента,[12] который присваивается телефону после первой связи с вышкой, и получения ей его IMSI. Делается это для того, чтобы уникальный идентификатор абонента меньше находился в эфире. Таким образом снижается вероятность его перехвата. Кроме того, отсылается IMEI — уникальный идентификатор мобильного устройства.[13] Этот идентификатор зашит в сам телефон. Благодаря этому возможно совершать вызовы экстренных служб даже с устройств в которых отсутствует SIM-карта. И соответственно, это также позволяет отслеживать такой телефон.

Также мобильный телефон может определять свое местоположение с помощью точек доступа Wi-Fi. Делать он это может за счет все той же триангуляции. Принципы такие же, как и в случае определения местоположения по вышкам сотовой связи.[14]

Еще телефон, конечно, может узнать свое местоположение с помощью GPS. Обычно под GPS понимают вообще систему спутниковой навигации.[1] Однако GPS, это конкретно американская система.[2] Наравне с ней сейчас также действует российская ГЛОНАСС,[3] европейская «Галилео»[4] и китайская «Бэйдоу».[5] Большинство телефонов сейчас используют гибридную систему навигации по спутникам, опираясь на данные всех спутниковых систем. Это позволяет значительно повысить точность определения местоположения. Благодаря анализам сигналов со спутников, точность определения составляет около одного метра. Еще раз подчеркиваю, что это

именно телефон, принимая и анализируя сигналы со спутников, определяет свои координаты. Самим спутникам он ничего не передает, и они его местоположение не знают.

Вот в общем-то и все способы определения местоположения телефона, как сетью, так и самим устройством. Многие, конечно, слышали еще байку о том, что отследить можно и выключенный телефон. С одной стороны, это действительно лишь байка, но с другой, возникшая не на пустом месте.

3 Отслеживание выключенного телефона в мифах и реальности

Отследить выключенный телефон можно в трех конкретных случаях. Первый, если телефон на самом деле не выключен. То есть, если в ваше устройство попало вредоносное ПО, которое при попытке выключить мобильник, лишь имитирует его выключение. А сам телефон при этом остается включенным, соединяется с базовыми станциями и даже может продолжать передавать информацию через Интернет разработчику этого вируса. Подобные средства использовали АНБ и ФБР.[6] Второй, если у вас особый телефон, который специально был разработан для шпионажа, в том числе в выключенном состоянии. Такие модели выпускались в разное время для спецопераций.[7] Третий, если ваш телефон был изменен аппаратно, либо программно (но в отличие от вируса, на уровне прошивки), что позволило ему осуществлять функции, способствующие его отслеживанию, даже после выключения. Вот и все ситуации, в которых может быть отслежен выключенный телефон. То что отследить можно любой выключенный телефон, миф. В выключенном состоянии телефон не отправляет и не принимает никаких сигналов, он обесточен.[8]

На это иногда слышится возражение, что телефон вовсе не обесточен, а убедиться в этом можно, установив будильник, который в нужное время зазвонит, даже если телефон будет выключен. В телефонах существует отдельный контур для питания часов и календаря.[9] Он никак не связан с радиомодулем и какими-либо адаптерами, поэтому говорить о том, что телефон по-прежнему полностью запитан не приходится. А заявления о том, что вся информация об устройстве мобильных телефонов, находящаяся в открытом доступе, не верна, а настоящая секретна, не выдерживают никакой критики. Сотовая связь и мобильники, это вещи вполне бытовые, а не какие-то секретные разработки, ими пользуются и их обслуживают самые обычные люди.

Россказни о секретности реального устройства и функций мобильников, о «спецсигналах», ни отмеченных ни в одной документации, для их удаленного управления, о поголовном молчании об этом операторов, о мировом сговоре производителей мобильников и спецслужб (причем всех стран, даже противоборствующих), это та же конспирология, не более содержательная чем домыслы, что Земля плоская, а от нас это скрывают, или что все беды России целенаправленно подстроены американцами, которыми управляют масоны, курируемые рептилойдами.

Личные истории, которыми изобилует Интернет, и статейки в газетах, не подкрепленные доказательствами в виде технической документации, о том, что отслеживание в выключенном состоянии возможно, всерьез воспринимать нельзя. А техническая документация на такую возможность нигде не указывает. [10]

Стоит ли в таком случае пренебрегать советом вынимать аккумулятор из устройства, когда вы хотите быть уверенны, что вас не отследят? Вовсе нет. Ведь если от обладания «особым» телефоном спасет проверка модели по спискам таковых, и отказ пользоваться телефонами, подаренными малознакомыми людьми, а от модификации на уровне аппаратного обеспечения и прошивки, вы защититесь, просто держа телефон всегда при себе, то от проникновения на него вируса, имитирующего выключение, не застрахован никто. Далее я дам рекомендации, следуя которым, вы серьезно снизите риск заражения вашего устройства.

Тот факт, что в современных смартфонах невозможно извлечь аккумулятор, часто звучит в качестве аргумента о возможности отслеживать любой выключенный телефон. Якобы именно для этого аккумулятор и сделали несъемным, чтобы устройство всегда было запитано. На самом деле причины такой конструкции экономические. Если пользователь не может извлечь аккумулятор, то в случае проблемы с ним, он не может самостоятельно заменить его и вынужден будет или покупать новое устройство, что выйдет дороже, или идти в специальную мастерскую, где с него возьмут деньги не только за сам аккумулятор, но еще и за работу по замене. А телефон, по всем нормам, обязан не излучать никаких сигналов, будучи не только выключенным, но даже просто поставленным в автономный режим. Этот режим порой так и называется «Режим полета», поскольку в самолете работающий телефон может привести к неприятностям. Точно также включенный мобильник может

привести к неприятностям находясь вблизи определенного медицинского оборудования. Именно поэтому устройство в ходе сертификации проходит различные тесты, в том числе, проверяется полнота деактивации в «Режиме полета» и при выключении. Если телефон полноценно не выключается и сохраняет способность отправлять и принимать сигналы, он не пройдет сертификацию. Так что выше названный аргумент тоже является не состоятельным.

С отслеживанием телефона полностью разобрались. Однако основная часть неприятностей, связанных с мобильными устройствами кроется в программном обеспечении смартфонов и планшетов. Об этом мы поговорим далее.

4 Общие уязвимости мобильных сетей

Мобильная сеть потенциально небезопасный канал связи. Широкий пласт атак возможно осуществить, эксплуатируя комплект протоколов ОКС 7 (SS7).[11]

Данный комплект протоколов обеспечивает само функционирование сотовой сети, т.е. является техническим каналом. Просто так им воспользоваться злоумышленнику не получится. Однако существует возможность подкупа сотовых операторов, взлома их оборудования, получения доступа к ОКС 7 шлюзу через услуги черного рынка в Интернете.

С помощью данного комплекта протоколов возможно отслеживать местоположение абонента, узнавать его идентификаторы, такие как IMSI, перехватывать и читать SMS. По результатам исследований, проведенных в 2015 году, все эти атаки были успешны в подавляющем большинстве случаев. Также примерно в половине случаев были успешны атаки, направленные на перенаправление и прослушивание входящих и исходящих вызовов, а также на изменение профиля абонента.[12]

Используя эти уязвимости, можно осуществлять атаки на аккаунты популярных мессенджеров, привязанные к номерам телефонов, таких как WhatsApp и Telegram.[13]

Известно, что злоумышленники уже давно успешно эксплуатируют данные уязвимости для обхода двухфакторной аутентификации и похищения денег с банковских счетов.[1]

Также сама по себе сотовая связь плохо защищена от прослушивания. В протоколы мобильной связи включено шифрование, однако зачастую оно очень

слабое.[2] И в случае простого перехвата сигнала, содержание разговора может стать доступным посторонним.

5 Общие уязвимости мобильных устройств

Помимо общих уязвимостей мобильной сети, существуют уязвимости, характерные для всех телефонов. Эти уязвимости кроются в прошивке самого процессора, управляющего радиомодулем. Начнем с того, что эта прошивка проприетарна, и свободных аналогов на сегодняшний день нет. Данная прошивка разрабатывалась для работы со стандартами, разработанными еще во времена, когда о защищенности связи никто особо не задумывался. Она спроектирована автоматически доверять всем командам, поступающим к ней. Конечно, комплекс команд стандартизирован, однако, это не исключает возможность наличия ошибок в коде, которые могут позволить заданные стандартами ограничения обойти. И существуют исследования, которые выявляли обилие ошибок, позволяющих удаленно выполнять вредоносный код.[3]

Эти уязвимости делают потенциально небезопасными все мобильные устройства. И хотя вероятность того, что они кем-то эксплуатируются крайне мала (использовать уязвимости на уровне приложений гораздо проще, чем на уровне встроенного ПО), необходимо помнить об их наличии.

6 Программное обеспечение мобильных устройств

Основная проблема, связанная с программным обеспечением мобильников, заключается в том, что по большей части оно не свободное. Многие смартфоны оснащены несвободной операционной системой. Это iPhone с ОС iOS, Windows Phone с ОС Windows Mobile, Blackberru со своей проприетарной системой. Такие устройства категорически неприемлемы для использования. Сложнее дело обстоит с системами Android. Сама по себе операционная система Android свободна, однако множество программ, поставляемых, с большинством ее сборок, например многочисленные приложения Google, проприетарны. Кроме того, проприетарны модули для многих частей оборудования, таких как радиомодуль, адаптеры Wi-Fi и Bluetooth. Последние представляют особую проблему, поскольку, как и в случае драйверов для части компьютерного оборудования, для них практически полностью отсутствуют свободные аналоги. Проприетарные же приложения, как правило имеют широкий доступ к

функциям устройства, для них характерен избыток разрешений. Уже упоминался пример с калькулятором. Калькулятор, это программа, которой в принципе не нужны никакие разрешения. Однако в Play-маркете есть множество калькуляторов, которые требуют доступ к Интернету непонятно для чего. Может быть и существуют разные объяснения наличию таких разрешений, но в любом случае, проверить функционал такого приложения не представляется возможным ввиду несвободной лицензии.

В связи со всем этим, в идеале, конечно, стоило бы использовать смартфон с полностью свободной системой, включающей свободные модули для аппаратных компонентов. Сейчас существуют и разрабатываются модели таких телефонов. Существуют также полностью свободные прошивки на базе Android. Однако, к сегодняшнему дню наблюдается острый недостаток таких прошивок. Тем не менее, далее в пособии я о них расскажу. А поскольку далеко не всем эти прошивки подойдут, расскажу как привести устройства с заводскими прошивками к максимально пристойному виду, и минимизировать риски.

7 Отслеживание между устройствами

Прежде чем переходить к рекомендациям, необходимо рассказать о еще одной проблеме, связанной со смартфонами и планшетами. Речь идет о так называемом отслеживании между устройствами — технологии, известной как cross-device tracking.

В свое время маркетологами была отмечена «проблема». Оказалось, что часто люди ищут информацию о товарах с телефона, а покупку осуществляют с компьютера, поскольку на маленьком экране мобильника это делать неудобно. Но в этом случае рекламные сети одного и того же пользователя, пользующегося разными устройствами, воспринимают как разных людей. И соответственно, целевая реклама, которая будет отображаться пользователю на смартфоне — на компьютере ему уже отображаться не будет. Соответственно, снижается вероятность того, что он приметит что-то еще для себя и не купит этого. Таким образом, остро встал вопрос о том, как отслеживать пользователей при использовании ими разных устройств. Конечно, когда пользователь на разных устройствах сидит с одного аккаунта, никаких проблем в идентификации нет. Но что делать, если он ищет что-то, не авторизуясь в своем аккаунте, а потом переходит на другое устройство? Как же применить

технологии манипуляции?

Способ слежки между разными устройствами был разработан, как уже было сказано, — он называется cross-device tracking. Еще часто можно встретить название ультразвуковой cross-device tracking. Суть данной технологии в следующем. Когда у пользователя на каком-то устройстве проигрывается рекламный ролик, этот ролик посылает ультразвуковой (пока будем называть его так) сигнал, который улавливает другое устройство пользователя и передает в некую структуру, корпорацию информацию о том, что владелец данного устройства смотрит такой-то ролик.[4]

С помощью данной технологии можно создавать отпечатки пользователя. Например узнавать, реагирует ли человек на рекламу, начинает ли что-то искать в интернет-магазинах или через поисковики в момент выхода рекламного ролика.[5]

Как не сложно догадаться, данная технология может быть использована не только корпорациями и их маркетологами, но и иными структурами в иных целях. Например взломщиками, в целях вычисления конкретного человека, для совершения в отношении него каких-либо злонамеренных действий. Или правительственными структурами с аналогичными намерениями. Может быть использована данная технология и для деанонимизации пользователей, применяющих инструменты туннелирования в своих Интернет-прогулках. К примеру, если вы настроили свою систему на компьютере в соответствии с той методикой, которая была дана выше, ваша система очень хорошо защищена даже от активного деанона. Тем не менее, может сложиться такая ситуация, что вы активировали какой-то скрипт на неком сайте, звук проигрался динамиком, другое ваше устройство — скажем, смартфон, лежащий рядом — уловил этот звук и передал злоумышленнику информацию о том, что владелец данного устройства совершал определенные действия на конкретном ресурсе.[6]

Эта коварная технология действительно существует и активно применяется. В сети можно найти статьи, в которых рассказывается о том, как полезна данная технология для различных компаний и даже предлагаются услуги по ее применению.[7] На том же YouTube можно найти презентации и вебинары сотрудников и почитателей таких корпораций как Google и Яндекс, которые во всю хвалятся тем, как успешно эти корпорации применяют данную технологию.

На первый взгляд, описание данной технологии выглядит как какая-то байка, поскольку заявление о воспроизведении ультразвуковых сигналов обычной техникой, которая заведомо не спроектирована для проигрывания звуков этого диапазона, звучит абсурдно. Но тут все не совсем так. Начнем по порядку. Человеческое ухо способно воспринимать звуки от 20 Гц до 20 кГц, соответственно техника проектируется для воспроизведения и приема звуков именно этого диапазона. То есть, именно ультразвук — то что выше 20 кГц — техникой, по идее, восприниматься не должен. Но тут есть пара моментов. То что границей воспринимаемых звуков является отметка в 20 кГц, не означает, что за ней сразу же все обрубается, просто по мере удаления частоты звука по ту сторону от этой границы, начинают лавинообразно нарастать искажения. Но техника, в принципе, способна воспринимать звуки большей частоты. Это первый момент. Второй момент, это то, что звуки вот этой верхней границы в 20 кГц очень мало кто действительно способен слышать. У большинства людей реальная граница проходит где-то в районе 18 кГц, а с возрастом, у пожилых людей эта граница может отодвинуться вообще до 11 кГц. То есть, звуки в диапазоне от 18 до 20 кГц очень мало кто услышит, и если поместить звук в эту область, он никем воспринят не будет, но техника его уловить способна. Таким образом, с технической точки зрения, осуществить «ультразвуковой» cross-device tracking действительно возможно. Правда корректней его было бы называть не ультразвуковым, а околоультразвуковым.[8]

В различных исследованиях расстояние на которое удавалось передать подобный сигнал от одного устройства к другому составляет от 30 сантиметров до 10 метров. Последнее, конечно, трудноосуществимо, но расстояние в несколько метров действительно покрывается. То есть, если смартфон лежит рядом, когда вы просматриваете что-то на компьютере, он вполне может воспринять сигнал, испущенный им, в результате попадания на такой вот звуковой маячок.

Для того, чтобы устройство передало информацию в корпорацию о том, что оно приняло этот сигнал и смогло передать персонифицированную информацию, информацию о владельце устройства, в этом устройстве должно быть установлено программное обеспечение, которое и будет осуществлять эту связь, — будет заставлять устройство принимать этот сигнал, обрабатывать, анализировать и передавать информацию разработчику этого ПО, или тому, чьи интересы обслуживает этот разработчик. Подобный функционал специально внедряется в программы корпораций. Естественно подобные программы являются сплошь проприетарными, и естественно, любая проприетарная программа потенциально может содержать в себе подобный функционал.

В некоторых публикациях, где рассказывается о cross-device tracking можно встретить заявления, что даже в случае, если отключить микрофон на устройстве, вы не можете защититься от cross-device tracking, поскольку звук способны воспринять динамики. Необходимо разобраться с этим вопросом, действительно ли динамики могут быть использованы в качестве микрофона.

Принцип действия динамиков и микрофона один и тот же, — мембрана микрофона толкает воздух, создавая его колебания, а мембрана динамика колеблется, под воздействием этих колебаний. То есть, потенциально они действительно могут быть взаимозаменяемы.[1] И существует исследование, в рамках которого была специально разработана программа, которая незаметно для пользователя меняла местами роли у микрофона и динамика, и в результате динамик начинал работать как микрофон. За счет этого возможно было осуществить прослушку.[2]

Как правило, опция смены функционала разъемов для динамика и микрофона находится на уровне чипсета. Производители чипсетов предоставляют драйвера для смены аудиоразъемов, причем это возможно осуществить не только в Windows, но и в GNU/Linux, с помощью программы hda-jack-retask.[3] Таким образом, на устройстве пользователя вполне возможно запустить вредоносную программу, которая произведет смену аудиоразъемов, и прослушка станет возможной не через микрофон, а через динамики.

Конечно нельзя сказать, что это возможно осуществить вообще в любых случаях с любыми динамиками. В случае с колонками, у которых крупные мембраны, это вряд ли сработает, потому что массивная мембрана колеблется с большим трудом, и ей воспринять звук будет достаточно тяжело. Но если говорить о тех динамиках, которые есть в смартфонах или наушниках, то с ними

получить хороший результат уже значительно проще. Но размер мембраны не единственное препятствие. Дело в том, что во многих динамиках стоят усилители, которые в обратную сторону звук не пропускают, и соответственно, с такими динамиками этот прием не сработает.[4] Таким образом, хотя качество воспринимаемого динамиками звука будет в любом случае хуже, чем у микрофона, но такое восприятие возможно, в том числе возможно и восприятие околоультразвуковых сигналов и, соответственно, осуществление cross-device tracking.

Некоторые авторы публикаций, рассказывающих об этой технологии, идут еще дальше и заявляют, что даже если полностью выпаить из смартфона не только микрофон, но и динамики, звук все равно может быть воспринят, при помощи гироскопа. Сначала давайте разберемся, возможно ли само по себе восприятие звука гироскопом смартфона.

Да, возможно, существует исследование, в котором было разработано программное обеспечение, которое использовало гироскоп для восприятия звука.[5] Частота опроса гироскопа составляет 200 Гц, она находится в рамках диапазона голоса человека. Поскольку в данном случае это частота дискретизации, ее необходимо поделить на два. Таким образом, воспринимаемая гироскопом частота звука будет находится в районе 100 Гц. Как отмечено в том исследовании, качество звука получается весьма плохим. Установить пол говорящего получалось в 84 % случаев, а отличить одного говорящего от другого из пяти человек в одной комнате удавалось лишь в 65 % случаев. Тем не менее, звук все-таки записывается, вполне возможно различить какие цифры говорит человек и отдельные слова. Таким образом, сама по себе прослушка с использованием гироскопа смартфона вполне возможна. Кто-то может заметить, что частота в 100 Гц воспринимается человеком как саб-бас. Скорее всего здесь была применена деконволюция — обратная свертка, т.е. восстановление цифровых сигналов, за счет которой возможно перевести то, что мы получили на выходе в то, что имело место на входе.[6]

Остается вопрос, возможно ли использовать гироскоп для cross-device tracking? Поскольку, как было сказано выше, частота звука, которую может воспринимать гироскоп составляет 100 Гц, а сигналы трекинга находятся в диапазоне 18–20 кГц, можно однозначно заключить, что нет.

Как можно защититься от этого типа слежки? В большинстве популярных статей, где о нем говорится, как правило приводятся совершенно экзотические

решения, вроде выпайки микрофона и динамиков, использование глушилки и т.п. Понятное дело, что для простого пользователя все эти варианты совершенно не серьезны. При этом методы, которые можно использовать для защиты от данной слежки, достаточно простые.

Если мы говорим о приеме этих сигналов, то он и последующая обработка могут быть осуществлены, конечно, разными устройствами, но повсеместно эту часть работы выполняют сугубо смартфоны и планшеты. То есть, в идеале, лучше полностью отказаться от смартфонов. Но это не всегда возможно. Поскольку программы, осуществляющие cross-device tracking сплошь проприетарные, полный отказ от такого ПО в пользу свободного является необходимым условием.

Если же говорить о воспроизведении этих околоультразвуковых сигналов, то если осуществляете веб-серфинг, просматриваете медиаконтент на компьютере (ровно как и на смартфоне или планшете), то используйте блокировщики рекламы и трекеров. Лучше всего применять блокировку скриптов. Также желательно не держать воспроизведение звука включенным постоянно, отключайте звук, когда не просматриваете медиаконтент. Дополнительно можно попробовать включить ограничение на воспроизведение звука в браузере. Ну а при просмотре ТВ-передач, во время показа рекламы также отключайте звук.

Вот такие вот незамысловатые советы. Мобильные устройства таят в себе и другие неприятности,[7] поэтому вопрос их правильной настройки и использования стоит крайне остро. Методика по такой настройке будет приведена далее в пособии.

3 Обеспечение безопасности на мобильном устройстве

8 Общие рекомендации по использованию мобильных устройств

Поскольку даже в случае использования полностью свободной системы на смартфоне, нет абсолютной гарантии от взлома (тем более, что существует проблема с реализацией виртуализации на большинстве мобильных устройств), я рекомендую разграничивать сотовую связь и Интернет-активность. То есть для обычных звонков и SMS лучше купить простой кнопочный телефон, а в качестве портативного устройства с функциями компьютера, приобрести

смартфон либо планшет. Используя для звонков и SMS обычный кнопочный мобильник, вы устраните риски, связанные со взломом через Интернет, для ваших контактов. Ну и также убережете от утечки на сторону содержание ваших телефонных разговоров и сообщений.

К сожалению, с кнопочными телефонами тоже не все просто. В немалом количестве моделей также присутствует вредоносный функционал. Например, многие из этих устройств передают данные при первом включении на сервера тех, кто разработал телефон или внедрил этот функционал на этапе транспортировки до места продажи. Эти данные могу включать в себя IMEI, IMSI, модель устройства, версию прошивки, страну, время активации, идентификатор базовой станции. Передача может осуществляться как через Интернет, так и обычным SMS, не отображаемым на устройстве. Есть и более вопиющие случаи, когда телефон автоматически подписывается на платные услуги, осуществляет звонки на платные номера и сливает данные пользователей на сторону, например, пересылает входящие SMS.[8] Проконтролировать этот момент практически невозможно. Иногда даже утверждается, что смартфоны более безопасны, поскольку их функционал легче контролировать, например, с помощью фаервола. Но когда дело касается обычной сотовой связи — несанкционированных звонков и SMS — никакой фаервол не поможет. Поэтому рекомендация использовать кнопочный телефон остается актуальной. Несколько снизить риски можно приобретая устройства крупных компаний, поскольку они чаще более ответственно относятся к работе с поставщиками, которые могут что-то внедрить в телефон, и кроме того, собирая информацию пользователей, хотя бы обеспечивают шифрование при передаче и хранении данных. Это ни в коем случае не значит, что крупные корпорации не собирают сведения, но хотя бы меньше риски того, что она попадет в руки мошенников. Желательно также перед покупкой прочитать отзывы об устройствах модели. Если они отсылают SMS на неизвестные номера или передают данные на какие-то сервера, это порой замечается пользователями и отмечается в отзывах. Также в качестве перестраховки можно после некоторого времени использования, запрашивать у оператора детализацию вызовов. Если в ней окажутся вызовы не инициализированные вами, то можно отказаться от данной модели телефона и искать другую. Еще можно порекомендовать первое включение телефона после покупки производить без SIM-карты. Это позволит предотвратить отправку информации

о том, где и когда телефон куплен, а также ту информацию об абоненте, которая содержится в SIM-карте. Это может не спасти в том случае, если в вирусе прописана отправка сведений после первого включения сугубо с SIM-картой. Но можно попытаться предотвратить это и в таком случае, дав телефону поработать какое-то время без SIM. Возможно, у устройства истечет время ожидания на отправку информации об абоненте. Что касается более серьезного вредоносного функционала, вроде принудительных платных подписок — слишком преувеличивать распространенность данной проблемы не стоит. По свидетельствам лаборатории Мегафона, подобный функционал присутствует только в моделях мелких фирм, неизвестных и недолговечных. К тому же, сейчас это явление становится все менее распространенным, производители начали стараться проявлять больше ответственности.[9] Также нельзя не упомянуть, что существуют проекты свободных кнопочных телефонов. На сегодняшний день, мне известен только один такой — Mudita Pure.[10] В нем используется свободная операционная система. Нет приложений для использования Интернета. Однако, есть функция VoLTE, и возможность использования протоколов, позволяющих передачу через Сеть, поскольку сейчас операторы сотовой связи активно используют именно их. Также присутствует возможность использовать его в качестве модема, при подключении по проводу. Также в нем присутствует GPS, что явно лишнее, — приложения карт на него не установишь, поэтому польза данного функционала едва ли есть. В его экране, кстати, используются жидкие чернила. К сожалению достать его проблематично, и стоит он как весьма продвинутый смартфон.

Что касается смартфона и планшета, то на них следует держать отключенными Wi-Fi, Bluetooth, геоданные, камеру и мобильный Интернет, когда эти функции не используются. А если вы, следуя данной выше рекомендации, не используйте это устройство для звонков и SMS, то его стоит вообще держать в режиме полета, всегда, когда вы не осуществляйте работу с сетью. Кроме повышения безопасности, это также серьезно снизит расход заряда батареи, а также сэкономит вам трафик, поскольку многие даже свободные приложения могут, работая в фоне, поддерживать связь с сетью. Также по возможности, стоит стараться держать отключенными камеру и микрофон, когда они не используются.

Здесь необходимо оговорить момент, что если вы используйте децентрализованные средства связи, которые требуют постоянного сетевого

соединения для синхронизации между собеседниками, то вам придется, конечно, держать включенным Wi-Fi либо мобильный Интернет, и соответственно, связь с сетью. Но в ином случае, постоянных соединений лучше избегать.

Таковы общие рекомендации. Пора постепенно переходить к конкретным инструкциям.

9 Схемы безопасности на мобильном устройстве

В качестве устройства для портативной Интернет-активности и осуществления других функций компьютера, в идеале, лучше использовать смартфон или планшет, который изначально разработан с ориентиром на безопасность и уважение к пользователю. Таковыми являются смартфоны Librem 5 и Necuno Mobile. Они спроектированы с изоляцией радиомодулей и адаптеров от носителей информации, с возможностью аппаратного выключения камер, микрофонов, адаптеров и радиомодулей. Librem 5 использует мобильную версию операционной системы PureOS, а также поддерживает некоторые мобильные версии GNU/Linux.[11] О них я расскажу далее. Necuno Mobile поддерживает большое количество мобильных систем GNU/Linux, а также наиболее свободную прошивку Android — Replicant.[12] О ней также речь пойдет в дальнейшем. К сожалению, достать такие смартфоны может быть не просто (в России они не продаются). И стоят они не дешево.

Менее радикальным вариантом является установка на обычное мобильное устройство одного из вариантов упомянутых выше мобильных версий систем GNU/Linux. В отличие от заводских прошивок Android, в них отсутствуют предустановленные несвободные прикладные приложения и библиотеки. Однако, прошивки для модулей все еще остаются проприетарными. Кроме того, есть и другая проблема. В отличии от компьютеров, на которые, в большинстве случаев, можно установить любую систему (при достаточном количестве ресурсов), мобильные устройства имеют весьма индивидуальные характеристики, и чтобы прошивке знать, как взаимодействовать с тем или иным устройством, ее нужно запрограммировать целенаправленно для него. Ввиду этого, такая прошивка может подойти не для каждого устройства. Например Plasma Mobile,[13] на момент написания пособия, подходит лишь для двух устройств.[1] Ubuntu Mobile примерно для десятка.[2]

Еще одним хорошим вариантом является также уже упомянутая прошивка Replicant.[3] У Replicant список поддерживаемых устройств очень ограничен.[4] Все они старые и ныне не выпускаются. Проблемой для создания версий под новые устройства является не только недостаток финансирования, но и конструкции новых устройств. Например в них радиомодуль может иметь прямой доступ к памяти, что неприемлемо для такой этичной и безопасной прошивки как Replicant.

Еще менее радикальным вариантом являются прошивки Android, в которых помимо несвободных модулей для различных компонентов оборудования содержаться также несвободные библиотеки. Тем не менее несвободные прикладные приложения в них отсутствуют. Наиболее популярной является прошивка LineageOS.[5] Она имеет версии для несравненно большого количества устройств, чем прошивки, о которых говорилось до этого. Тем не менее, список все же ограничен.[6] Помимо LineageOS существуют также прошивки Paranoid Android,[7] Omniram[8] и /e/.[9] Однако у них более скудные списки поддерживаемых устройств. Помимо того, что не каждое устройство подходит для перепрошивки, еще одной ее проблемой является то, что она может закончиться не установкой новой прошивки, а тем, что устройство превратиться в кирпич. Понятное дело, что если у вас дорогое устройство, вы можете не решиться рисковать убить его, в попытке поставить что-то более свободное, при том, что уровня свободы и безопасности, какого вы можете достигнуть на компьютере, на мобильном устройстве вы в любом случае не получите.

Поэтому для такой ситуации можно порекомендовать оставить заводскую прошивку и получить root-права. Права суперпользователя в Android имеют то же значение, что и в GNU/Linux. Они фактически дают вам полный контроль над устройством, позволяют вносить системные изменения. Для простого обывателя они дают две вещи. Во-первых, это возможность полноценно удалить предустановленные несвободные приложения. Во-вторых, использовать полноценный файервол. Приложения можно удалить и без root-прав, однако такое удаление будет неполноценным. Файервол же без прав суперпользователя возможно использовать, но это будет уже не полноценный сетевой экран, который отнимет у вас некоторые возможности, о чем я расскажу далее. В Сети написано очень много ерунды про то, что получать права root опасно. Если у вас есть голова, и вы не будите бездумно нажимать «Да» в сообщении

«Предоставить права суперпользователя приложению?», и к тому же будите устанавливать только свободные программы, то вам бояться нечего. К сожалению, получение root-прав тоже не лишено своих проблем. Во-первых, при рутировании также существует риск превратить устройство в кирпич. Здесь этот риск крайне незначителен, в отличие от случая перепрошивки, однако потенциально он существует. Во-вторых, имея root на устройстве, вы возможно, не сможете больше обновлять прошивку стандартным способом. При попытке произвести обновление вам будет заявлено, что была произведена несанкционированная модификация системы. С какой радости действия над устройством, за которое вы отдали деньги, а значит оно, вроде как, принадлежат вам, требуют каких-то санкций, непонятно. Вернее понятно, недобросовестные разработчики опять пытаются расширить свою власть над пользователями, наглея все более и более. В-третьих, вы возможно, не сможете пользоваться некоторыми сервисами, например бесконтактной оплатой или проездом с помощью технологии NFC.[10] Опять же, вам стараются перекрыть как можно больше контроля в вашей собственной жизни, поскольку это выгодно корпорациям и государствам. Насчет обновления и NFC существует возможность скрыть факт наличия root и за счет этого все-таки воспользоваться этими возможностями. Но что касается бесконтактной оплаты, то я вообще не рекомендую ей пользоваться, поскольку это дополнительный канал слежки. Несмотря на то, что root-права, это очень хороший вариант, поскольку риски и ограничения крайне незначительны, все же кого-то они могут отпугнуть. Также существует вероятность, что получить root просто не получится.

Если очень опасайтесь навредить своему устройству или потерять возможность обновлять прошивку, или же у вас просто-напросто не получится получить root, то есть еще один вариант. Это просто удалить все какие возможно несвободные приложения, те что не удаляются, отключить, а тем, что останутся активны, не давать сливать информацию, перекрывая им доступ к Интернету. Существуют сетевые экраны, работающие без root-прав. Они формируют локальный VPN (не подключение к удаленному серверу, а поднятие его непосредственно на устройстве для личных соединений), который фильтрует трафик приложений. За счет этого доступ к сети можно позволять только тем программам, которым нужно. Таким образом, каналы слива информации проприетарными приложениями будут перекрыты.

Вот все схемы безопасности на мобильном устройстве. Как вы видите, ситуация со смартфонами и планшетами очень печальна. На тех устройствах, что доступны широкому пользователю невозможно получить тот уровень свободы, что на компьютере, невозможно полностью вернуть себе контроль над своими вычислениями. Тем не менее, кое-что предпринять для достижения безопасности все-таки можно. Но безусловно, необходимо гораздо большее. Пока же нет таких возможностей, придется следовать тем или иным имеющимся схемам безопасности.

10 Рекомендации по подбору устройства

Несмотря на то, что на Android безопасность в немалой степени достижима, все же у разных устройств, возможности для этого разные. Рекомендовать что-то конкретное для приобретения довольно сложно. Однако можно сказать что не следует приобретать. Категорически не следует приобретать устройства от ZTE и Huawei. Как указывают различные свидетельства, оборудование этих компаний нашпиговано закладками.[11] Также не следует брать устройства Xiaomi. В них также присутствуют закладки и уязвимости.[1] К тому же, если вы приобретете такое устройство с заблокированным загрузчиком, то для его разблокировки вам потребуется связываться с производителем и просить у него разрешения это сделать.[2] Подобная политика, верх наглости. Вроде как вы приобрели устройство, заплатили за него деньги, но оно вам фактически не принадлежит, вы должны еще спрашивать разрешения, чтобы что-то с ним сделать. Политика обычная для компаний, разрабатывающих несвободное ПО и не уважающих своих клиентов. Разблокированный загрузчик же необходим как для перепрошивки так и для получения root-прав.

Также проблема с разблокировкой загрузчика есть у устройств Motorola.[3] С ними вам также придется спрашивать разрешения у производителя. Кроме того, у устройств этой компании также выявлялись уязвимости.[4] Аналогичные проблемы у устройств LG,[5] HTC[6] и Sony.[7]

Также не рекомендую Samsung, поскольку есть сведения, что они также движутся в направлении усложнения разблокировки загрузчика.[1] Кроме того в них не единожды обнаруживались уязвимости.[2] Отмечалось, что имеет место намеренное замедление работы на старых моделях, чтобы заставить

пользователей чаще покупать новые.[3]

Также проблематична ситуация с некоторыми моделями Lenovo. Среди них есть те, у которых разблокировка загрузчика имеет аналогичные проблемы.[4] Кроме того в устройствах этой компании также находили вредоносные особенности.[5]

Что касается того, какие устройства можно порекомендовать, то тут все достаточно сложно. Очень много новых производителей, про которых мне ничего не известно. Из тех достойных, что еще встречаются в магазинах можно отметить BQ, OnePlus и Wileyfox. Как ни странно, хороши устройства от Google.

Далее я дам общие схемы по перепрошивке устройств и получению на них root-прав. Конечно, речь идет только о телефонах на базе открытых систем, таких, как Android. Если у вас, к примеру iPhone, от такого устройства следует избавляться. На нем вы не получите и тени безопасности. В очередной раз повторяю, в проприетарной системе, такой как iOS, этичностью и не пахло. Использование несвободных компонентов, драйверов и модулей, это крайняя вынужденная мера. Это изъян, и его допущение может быть вызвано только безысходностью. Если есть возможность начать использовать устройство лишенное таких изъянов, ею следует воспользоваться. Если же такой возможности нет, приходится переходить к другим схемам.

11 Разблокировка загрузчика и установка кастомной рекавери

Прежде чем перепрошивать устройство или получать права root, необходимо разблокировать загрузчик.

Перед разблокировкой обязательно сделайте запасную копию данных. А вообще в очередной раз говорю, никогда не храните никакую информацию в единственном экземпляре.

В настройках, в разделе «О телефоне» или «Об устройстве» необходимо от 5 до 10 раз нажать на «Модель» или «Номер сборки». После этого внизу появится сообщение, что вы стали разработчиком. Раздел «Для разработчиков» появится либо непосредственно в разделе «О телефоне» либо просто в меню настроек. Идем в него и там активируем OEM-разблокировку, а также отладку по USB.

Далее вам понадобится установить на компьютер программы adb и fastboot. Они есть в репозиториях Trisquel. После их установки, подключаем смартфон

или планшет к компьютеру, открываем терминал, набираем sudo bash, а затем пароль. Все действия выполняются с правами суперпользователя.

После этого вводим команду

```
adb reboot bootloader
```

Это переведет смартфон в режим загрузчика. Если команда не срабатывает, то необходимо иным образом открыть загрузчик. На разных устройствах это происходит по разному. На одних необходимо зажать кнопку увеличения громкости и включения, на других обе кнопки громкости и включения.

После того, как устройство перейдет в режим загрузчика необходимо удостовериться, что компьютер его видит. Для этого набираем команду

```
fastboot devices
```

В терминале отобразится код устройства, который также отображается на экране смартфона или планшета. Если все так, то вводим команду

```
fastboot oem unlock
```

Если после этого устройство не перезагрузится автоматически, перезагрузите его. Загрузчик должен быть разблокирован.

После этого необходимо снова включить отладку по USB. Далее, как для перепрошивки, так и для рутирования необходимо установить кастомное рекавери. Наиболее предпочтительной является рековери TWRP,[6] которое нужно скачать отдельно.[7]

Переходим в режим загрузчика, уже известным способом, подключаем смартфон к компьютеру, если не подключен, проверяем, видит ли компьютер наше устройство, и набираем команду

cd **/home/user**

Жирным шрифтом выделен путь к папке, где лежит, скачанный файл рекавери (не забудьте перенести его из виртуалки в основную систему), вам необходимо прописать свой. После этого вводим команду

fastboot flash boot **recavery**.img

Жирным шрифтом выделено название файла рекавери. У вас оно будет другим, его и необходимо вписать.

Когда процесс установки закончится можно перезагрузить устройство. Теперь на нем есть рекавери, с помощью которого можно установить другую прошивку или получить root-права.

12 Установка прошивки

Для начала необходимо прошивку скачать и перенести в основную операционную систему. Обращаю внимание, что файл прошивки должен иметь расширение zip.

Чтобы установить прошивку, необходимо войти в рекавери. Для этого можно набрать команду в терминале на компьютере, когда смартфон подключен к нему

fastboot boot **recavery**.img

Жирным шрифтом выделено название файла рекавери. У вас оно будет другим, его и необходимо вписать. Если команда не сработает, то необходимо войти в нужный режим другим способом. На многих моделях для этого нужно зажать кнопку громкости вниз и включения.

Когда рекавери откроется, нажимаем Wipe. После этого нажимаем Format Data. Это удалит шифрование и все данные на устройстве.

Затем возвращаемся в предыдущее меню и нажимаем Advanced Wipe, затем выбираем системный раздел и нажимаем Swipe to Wipe.

После этого, на устройстве выбираем Advanced, затем ADB Sideload и проводим пальцем внизу, для запуска загрузки прошивки. На компьютере набираем команду

adb sideload **filename**.zip

Жирным шрифтом выделено название файла прошивки. У вас оно будет другим, его и необходимо вписать. После того, как завершится установка прошивки, перезагружаем устройство. На этом перепрошивка закончена.

13 Получение root-прав

Как и для перепрошивки устройств, существует общая схема получения прав суперпользователя. По сути, это единственная схема, поскольку все остальные связаны с использованием сомнительных проприетарных программ, требующих доступа к Интернету и памяти устройства. Например программа Kingo Root способна рутировать большое количество моделей, при этом она требует, чтобы был включен Интернет на устройстве, и явно передает какие-то данные. Еще более сомнительная программа King Root. Она более простая, но помимо того, что она несвободна и также, видимо, ворует данные, она еще и может в случае неудачного рутирования, вовсе убить ваше устройство.

Перед рутированием обязательно сделайте запасную копию данных.

Существуют различные инструменты для рутирования. Наиболее предпочтительным является Magisk. Она свободна, не вносит изменений непосредственно в операционную систему, за счет чего существует возможность скрыть ее использование. Все это выгодно отличает ее от популярного инструмента SuperSU, который проприетарен и вносит серьезные изменения непосредственно в систему. Его я ни в коем случае не рекомендую использовать.

Скачиваем apk-файл Magisk Manager (это программа для управления root-правами) и zip-архив Magisk и перебрасываем файлы на устройство, которое собираемся рутировать.[8] После этого открываем файловый менеджер, находим Magisk Manager, нажимаем на него и устанавливаем.

Затем заходим в рекавери. Для этого на многих устройствах необходимо нажать кнопку громкости вниз и включения, но у вас возможно это осуществляется по-другому. В рекавери нажимаем Install и выбираем файл Magisk. После чего проводим пальцем внизу экрана. Когда установка закончится можно перезагрузить устройство.

После перезагрузки, открываем Magisk Manager и проверяем наличие root. После этого необходимо войти в настройки приложения и деактивировать параметр Magisk Hide. Иначе root слетит после следующей перезагрузки устройства. После этого можно закрыть менеджер root-прав.

В не зависимости от того, удалось вам рутировать устройство или нет, следующим шагом является замена проприетарных приложений свободными.

14 Установка и использование F-Droid

Первым делом я рекомендую даже не начать удалять нежелательные приложения, а скачать и установить этичный магазин приложений. Play-маркет и сам по себе проприетарен, и содержит кучу несвободных приложений, не подпадающих под вменяемые критерии безопасности. К тому же для использования он требует регистрации. Этичной заменой этой помойки является магазин приложений F-Droid.[9] Он свободен и его репозитории содержат только свободные программы. Перед включением нового приложения в них, оно проверяется на уязвимости и сомнительный функционал. Если программа имеет в своем функционале слежку, поддержку несвободных дополнений, использование несвободных сервисов и другие неприятности, оно может быть включено в репозитории, однако его страница будет содержать соответствующие предупреждения. Устанавливая программы только из F-Droid вы будите избавлены от проприетарного ПО, а при попытке установки приложения с сомнительным функционалом, будите о таковом предупреждены. Скачивайте себе на устройство apk-файл с официального сайта и устанавливайте.[10] У F-Droid есть и альтернативы. Это магазины G-Droid,[11] M-Droid[12] и Foxy Droid.[13] Они менее развитые, но могут стать вариантом для тех, у кого возникнут проблемы с установкой и использованием F-Droid. Если же вам не повезет и F-Droid вообще откажется устанавливаться или будет работать не корректно, и аналогичные проблемы возникнут с альтернативными магазинами, то в этом случае вариантом может стать установка нужного софта непосредственно с официального сайта F-Droid.

15 Установка клавиатуры и браузера

В большинстве заводских сборок Android в качестве клавиатуры установлена клавиатура от Google. Она проприетарна и скорее всего является кейлогером. То есть она запоминает все ваши нажатия клавиш и отправляет эту

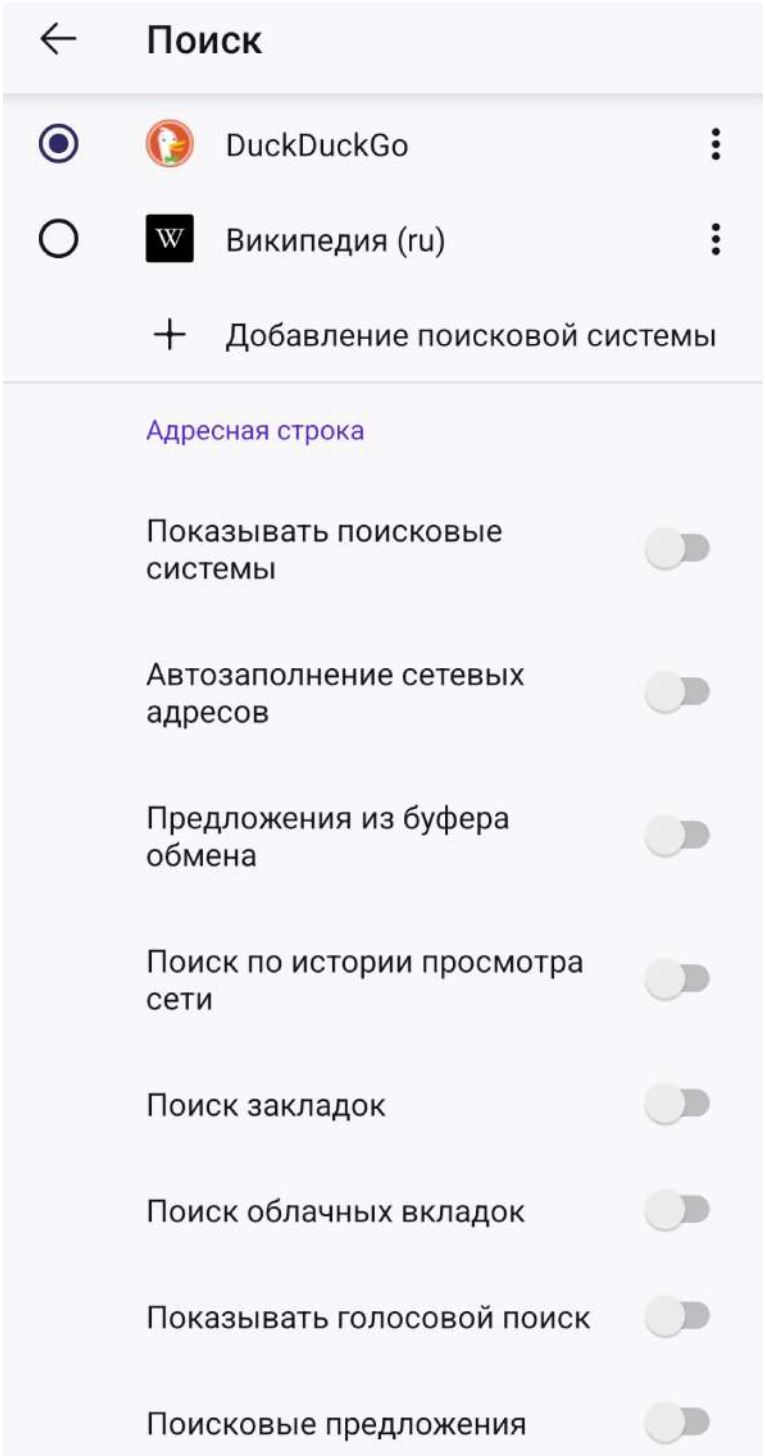
информацию Google. Это очень серьезная уязвимость, и ее необходимо устранить, заменив эту клавиатуру на что-то более этичное. В репозиториях F-Droid есть несколько клавиатур. Наиболее удобной и функциональной из них является AnySoftKeyboard.[14] Устанавливаем ее, а также русскую локализацию.[1] После этого ищем иконку данной клавиатуры в меню смартфона/планшета, нажимаем на нее и производим настройку. Она интуитивна, Меню само ведет вас по нему. После настройки закрываем приложение. Теперь данная клавиатура установлена у вас по-умолчанию.

Поскольку во время чистки может возникнуть необходимость что-то узнать в Интернете, я рекомендую следующим установить браузер. Понятное дело, что предустановленные проприетарные браузеры, типа Google Chrome, не подходят для использования.

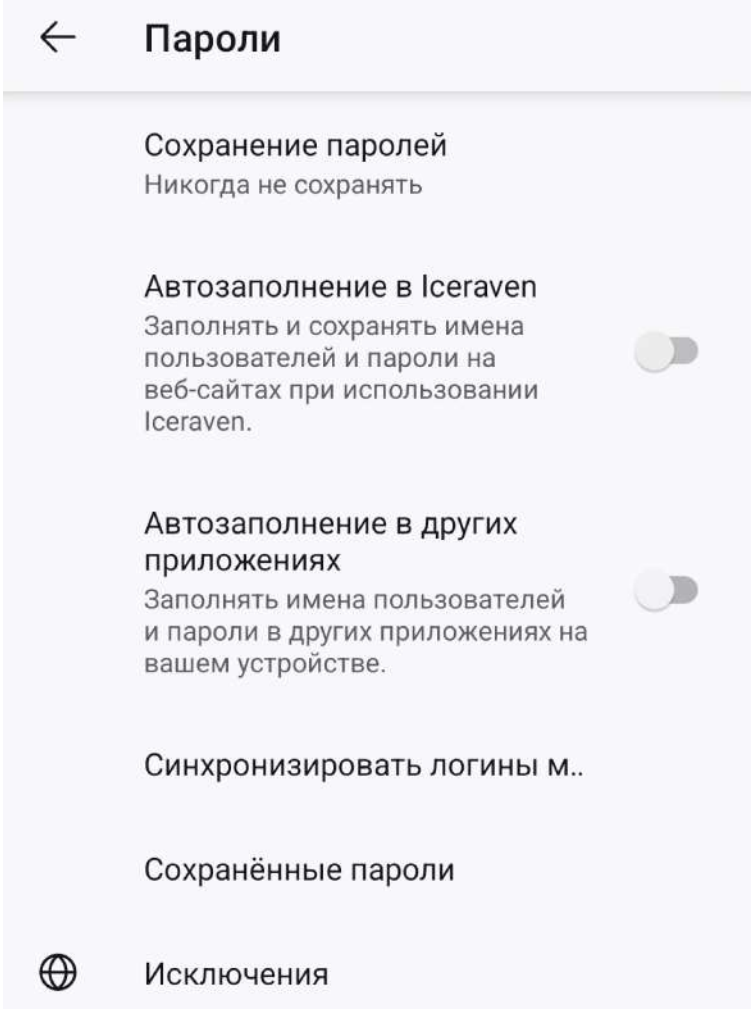
В F-Droid много браузеров. К сожалению, большинство из них блеклые и не имеют гибких настроек безопасности. Однако, в F-Droid есть программа, в которой присутствует ряд интересных браузеров, среди которых есть то, что нам нужно. Программа называется FFUpdater.[2] Устанавливаем ее. Открываем и нажимаем значок плюс в оранжевом кружке справа на пересечении синего и белого полей. Выскочит список доступных браузеров. В качестве основного браузера я рекомендую использовать Iceraven Browser. Он имеет достаточно неплохие настройки безопасности, подобные классическому Firefox, также позволяет устанавливать различные расширения. Однако, в целом, его настройки приватности более жесткие чем у Firefox, кроме того он позволяет редактировать глубинные настройки конфигурации, что более не позволяет делать классическая версия Firefox. Нажимаем на Iceraven. Откроется окно, в котором будет отображена ссылка и шкала загрузки. Если при этом само скачивание не началось, то ссылку необходимо скопировать в имеющийся браузер и через него скачать установочный файл Iceraven. Когда файл будет скачан, выскочит уведомление с предложением его установить. Нажимаем «Установить». После того как браузер будет установлен, скачанный apk-файл можно будет удалить, а Iceraven нужно будет настроить.

Запускаем его. Вначале выбираем его вид, какой больше нравится, а также уровень защиты приватности. Для корректного открытия страниц лучше выбрать обычную. После чего нажимаем внизу синюю кнопку «Начать просмотр сети». Теперь нажимаем три точки справа внизу или вверху, в зависимости от того, какой вид выбрали, и идем в «Настройки».

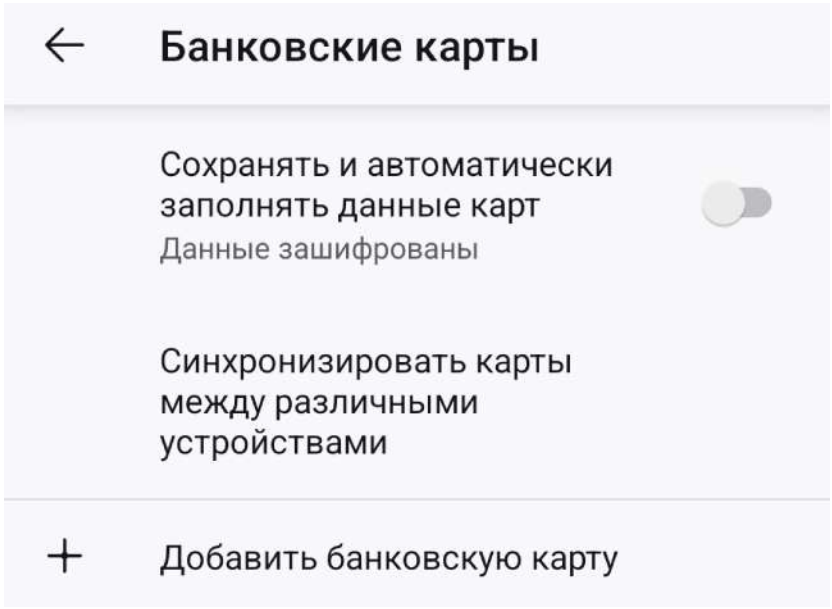
Здесь идем в «Поиск» и удаляем все кроме DuckDuckGo и Википедии, для чего нажимаем на три точки справа от плагина и выбираем «Удалить». Затем в разделе «Адресная строка» деактивируем все ползунки.



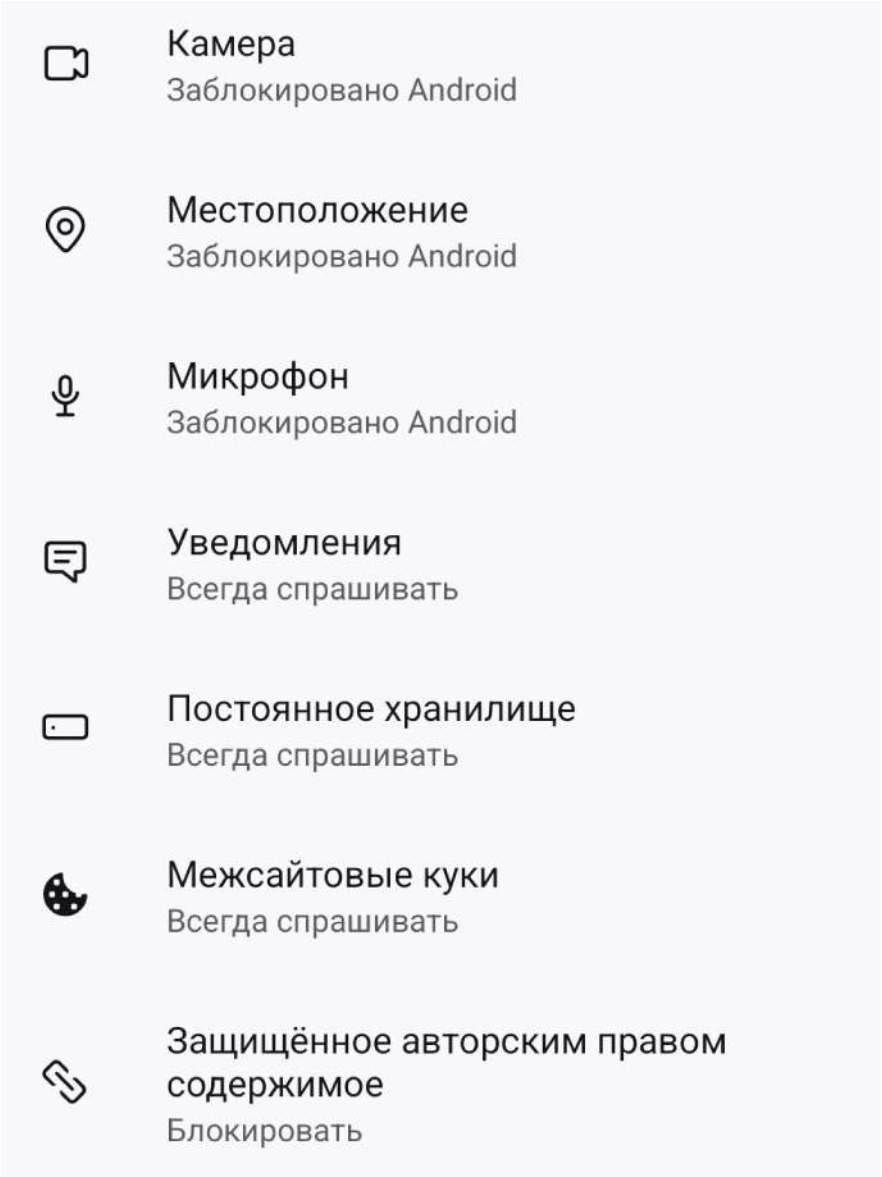
Возвращаемся назад и идем в «Пароли». Здесь нажимаем на «Сохранение паролей» и выбираем «Никогда не сохранять». Также деактивируем «Автозаполнение в Iceraven».



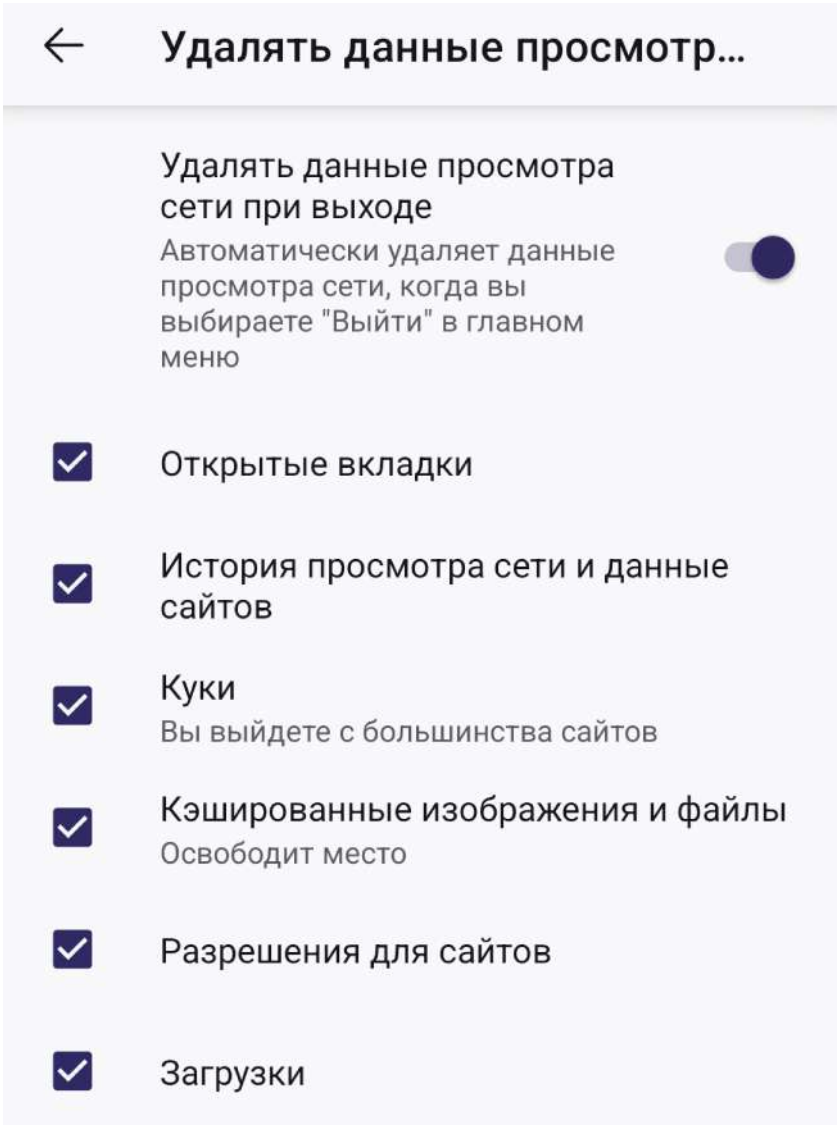
В категории «Банковские карты» деактивируем «Сохранять и автоматически заполнять данные карт».



В категории «Разрешения сайтов» проверяем, чтобы были заблокированы камера, микрофон, местоположение и DRM.



В категории «Удалять данные просмотра сети при выходе» активируем удаление и проставляем все галочки.



Перезапускаем браузер и набираем в адресной строке about:config. Настройка глубинной конфигурации аналогична настройке на компьютере. Однако помимо уже известных функций также следует отключить еще несколько.

device.camera доступ к камере.

dom.battery.enable доступ к данным об уровне заряда батареи.

После перезапуска браузера, следует установить уже известные расширения https everywhere, noscript и user agent switcher. К сожалению, для мобильного браузера нет возможности установить зашумитель отпечатка canvas defender fingerprinting. Но можно установить его блокировщик, canvas blocker. Также можете установить privacy badger или privacy possum. Настройку белого списка noscript, пока на вашем устройстве куча несвободного ПО, можно отложить.

Что ж, устройство готово к чистке. Пора удалять проприетарные программы.

16 Удаление и отключение вредоносных программ

Если вы получили root-права, то первым делом устанавливайте из F-Droid программу Batch Uninstaller.[3] Она позволяет удалять даже те приложения, которые невозможно убрать обычным способом. Программе нужно будет предоставить root-права. Если данная программа работает некорректно, то можете попробовать /system/app mover.[4] Если же и она не удаляет приложения, то можно использовать файловый менеджер Amaze.[5] В этом случае, в нем необходимо войти в раздел App Manager.

Если же root-прав нет, то открывайте настройки и идете в раздел с приложениями. Здесь вы также будите удалять сомнительные программы. Если не выходит удалить ту или иную программу, то отключайте ее. Если нет функции отключить, то запретите ей доступ ко всем функциям устройства, включая Интернет. Опять же это не для всех приложений окажется возможным. В дальнейшем я расскажу о способе удалить без root-прав и эти приложения. Также далее я расскажу о настройке файервола, который не даст им сливать ваши личные данные.

Начинаем избавляться от потенциально вредоносных программ. В первую очередь это все, имеющее в названии слово «Google». Исключение составляют «Сервисы Google Play», поскольку без них могут пропасть некоторые функции, например отправка SMS. Естественно, удалить нужно различные клиенты для социальных сетей, таких как VK и Instagram. Если вам не жить не быть нужны эти сервисы, лучше пользуйтесь ими через браузер или свободные клиенты (для некоторых соц. сетей такие есть, о них расскажу в дальнейшем). Также удаляем предустановленные прикладные приложения, такие как браузер, приложения для заметок, галерею, калькулятор, диктофон, программы для чтения документов, для управления камерой и т.д. Сложнее все с системными приложениями. Необходимо быть очень осторожным и внимательным, чтобы не удалить то, без чего ваше устройство потеряет важные функции. Лучше такие приложения вообще не трогать, за исключением тех, что имеют в названии слово Google, не считая, уже упомянутых «Сервисов Google Play». Ни в коем случае не удаляйте «телефонные» приложения, приложения для SMS и контактов. Иначе все эти функции могут просто пропасть. Например, если

удалить приложение для совершения звонков, может пропасть определение сети, и станут невозможными звонки, SMS и подключение к мобильному Интернету. Однако такие приложения можно попробовать отключить, это далеко не всегда вызывает проблемы. Если не выходит отключить их обычным способом, в помощь приложение Activity Launcher.[6] В нем среди приложений нужно найти «Настройки», в них «Управление приложениями» или «Приложения» и там произвести отключение.

Если не пользуйтесь NFC-технологиями, к примеру, оплатой через терминал с помощью телефона, можете удалить приложение «Брелок». Вообще используя подобные технологии, вы серьезно снижайте свою безопасность, о чем я уже говорил.

Возможный шпионаж оставшихся приложений будет предотвращать файервол. О нем мы поговорим отдельно.

17 Удаление приложений без root-прав

Существует способ удалить приложения, для которых функция удаления и даже отключения неактивна, без прав суперпользователя. Однако, как я уже говорил, такое удаление будет неполноценным. Объем свободной памяти устройства, как правило, не увеличивается, а значит данные удаленных таким способом приложений по-прежнему остаются. Кроме того, они продолжают фигурировать в списке приложений в настройках, хоть и с пометкой «Не установлено» или «Отсутствует». Тем не менее, таким способом можно удалить не только те программы, от которых невозможно избавится обычным способом, но и те, которые невозможно даже отключить при помощи функций самого устройства.

Для этого понадобится компьютер с установленным инструментом adb, о котором уже говорилось. Также необходимо активировать отладку по USB на устройстве, что также уже описывалось выше.

Подключаем смартфон к компьютеру и набираем команду в терминале с правами суперпользователя

```
adb shell pm uninstall --user 0 failname
```

Жирным шрифтом выделено название приложения. Вместо него необходимо указать то, которое хотите удалить вы. Если не знаете полное

название приложения, можете воспользоваться программой App Manager.[7] В ней отображаются приложения с полными названиями.

Данную команду необходимо прописать для каждого приложения, которое хотите удалить.

18 Шифрование устройства

Одним из наиболее серьезных способов защитить свои данные, является шифрование устройства. Функции такого шифрования находятся в Настройках, обычно в разделе «Безопасность» или «Конфиденциальность». Из способов шифрования я рекомендую выбирать шифрование с помощью пароля. Рекомендации по составлению пароля такие же, как для компьютера. Не рекомендую использовать тот же самый пароль. Одинаковые пароли допустимы лишь в рамках одного устройства. Поскольку методика шифрования также индивидуальна для каждого устройства, я не могу дать единой инструкции. Обычно в Меню по шифрованию все интуитивно, просто следуйте подсказкам и вы все сделайте сами.

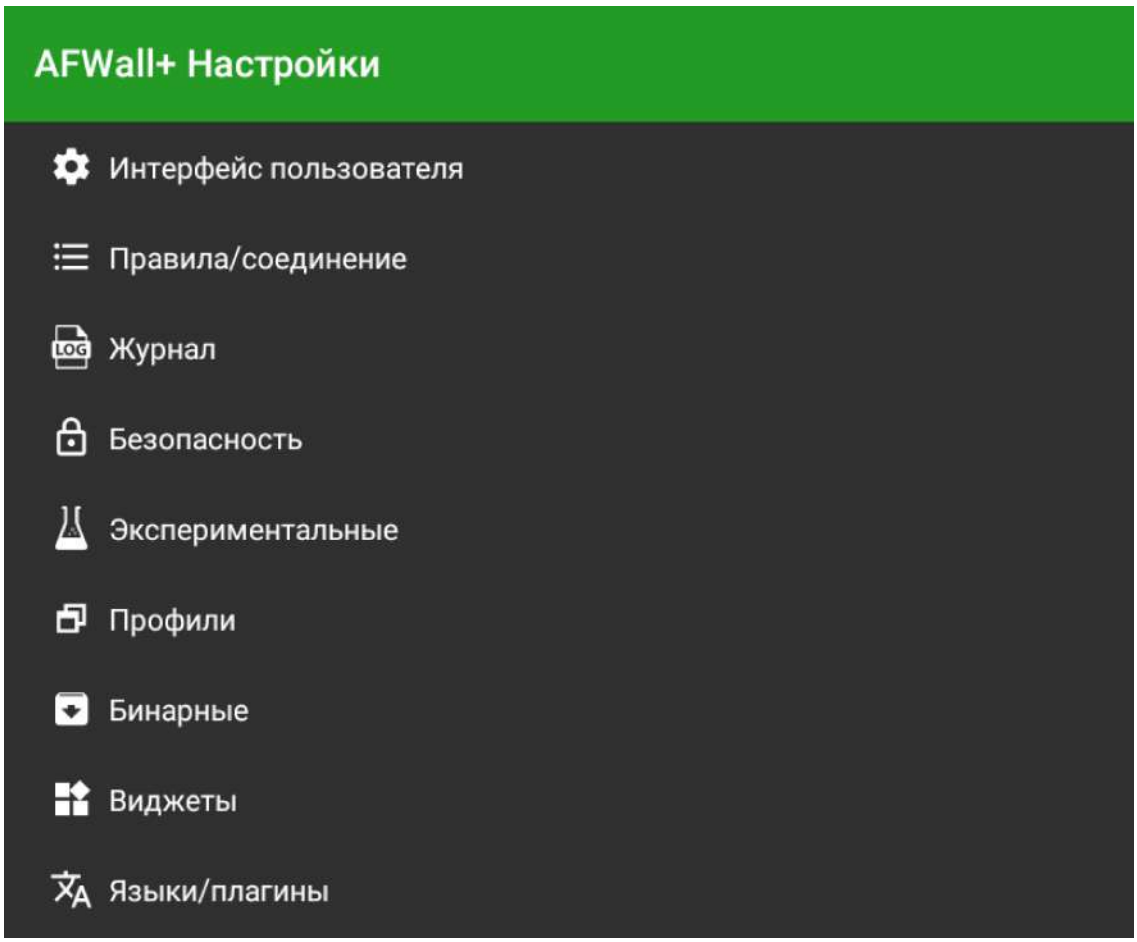
Также рекомендую зашифровать карту памяти, если она присутствует в устройстве.

Обращаю внимание, что не на всех устройствах и не всегда шифрование работает корректно. Иногда даже после его включения, данные на устройстве могут остаться не зашифрованными. Кроме того, чем старше устройство, тем шифрование менее надежное. Учитывайте это, однако, помните, что слабое шифрование лучше чем вообще никакого.

19 Установка и настройка AFWall+

Если у вас есть root-права, вы имейте возможность использовать полноценный файервол, вносящий изменения непосредственно в сетевой фильтр устройства. Если root нет, то вам необходима другая программа, о которой я расскажу отдельно. Сейчас же пойдет речь о полноценном файерволе. Таковым является приложение AFWall+.[8] Устанавливаем его.

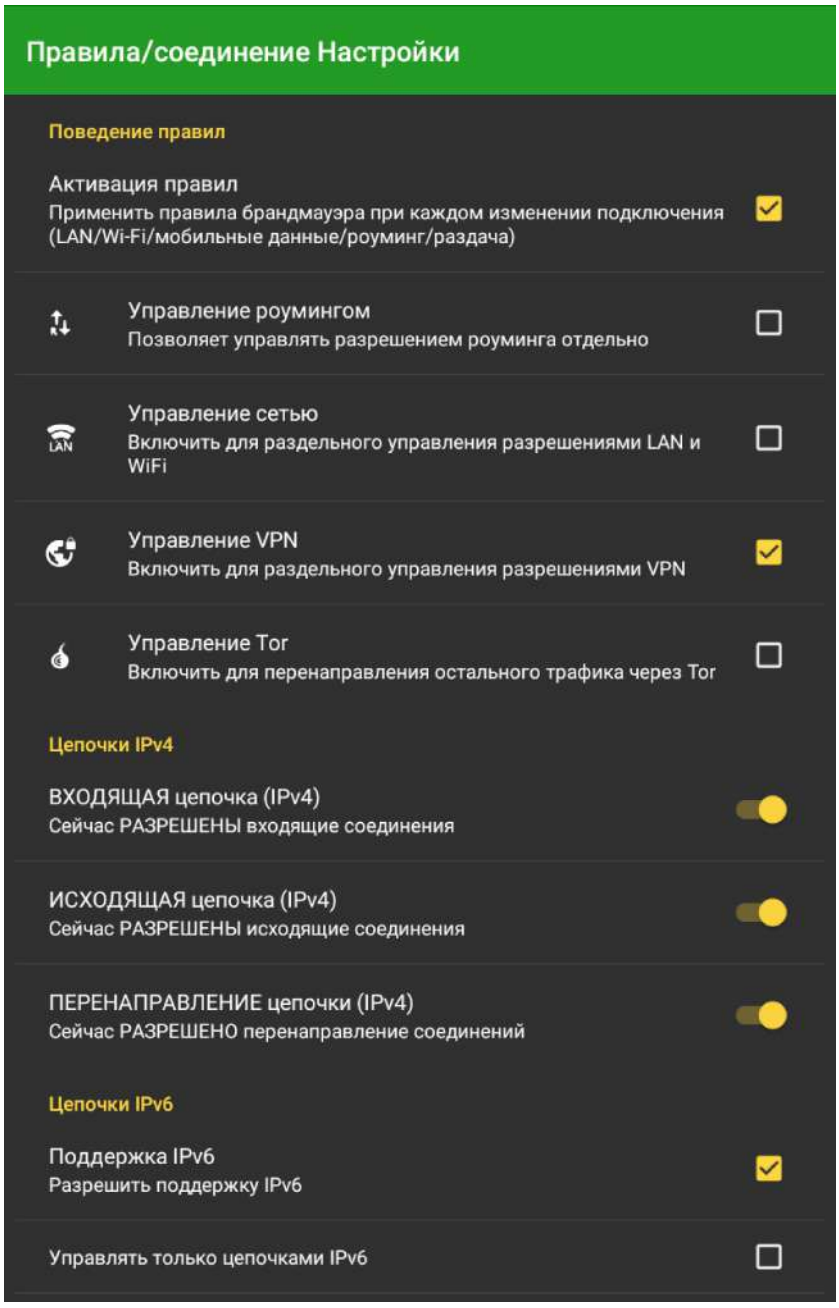
После установки, открываем приложение и идем в настройки. Для этого нажимаем три точки справа сверху и выбираем «Настройки».



Категория «Интерфейс пользователя», как ясно из названия, настраивает интерфейс, то как будет выглядеть приложение. Тут меняйте что-то по своему усмотрению.

В категории «Правила/соединение» ставим галочку на «Активация правил». Если вы сталкивайтесь с роумингом и хотите сэкономить, перекрыв доступ к Сети приложениям, которым вне роуминга позволяйте есть трафик, то можете поставить галочку на «Управление роумингом» и тогда для этого случая задать отдельные правила. Если приходится подключать устройство к беспроводной локальной сети и при этом вы хотите, чтобы какие-то приложения, которым не позволено использовать Интернет при Wi-Fi-подключении, могли использовать подключение к локальной сети или наоборот, поставьте галочку на «Управление сетью». Если намерены использовать VPN, в качестве которого на мобильном устройстве может выступать и Tor (позже я объясню, что это значит), то ставьте галочку на «Управление VPN» и тогда у вас появится возможность определенным приложениям иметь доступ к сети только через VPN. «Управление Tor», это попытка пустить трафик приложений, у которых в настройках нет интеграции с сетью Tor, через нее. Успех, к сожалению, не гарантирован. Кроме того, при

этом происходит утечка DNS, что делает использование этой функции бессмысленным.[9] В AFWall+ есть возможность прописывать свои правила непосредственно в инструмент iptables. Используя этот функционал, можно настроить принудительное использование Tor без утечек DNS. Однако, это под силу только продвинутым пользователям, поэтому данный вопрос оставляем в стороне. В графе «Цепочки IPv4» активируем все ползунки. В графе «Цепочки IPv6» можем активировать поддержку IPv6. Но галочку на «Управлять только цепочками IPv6» не ставим. Нам нужно контролировать и IPv4 трафик.

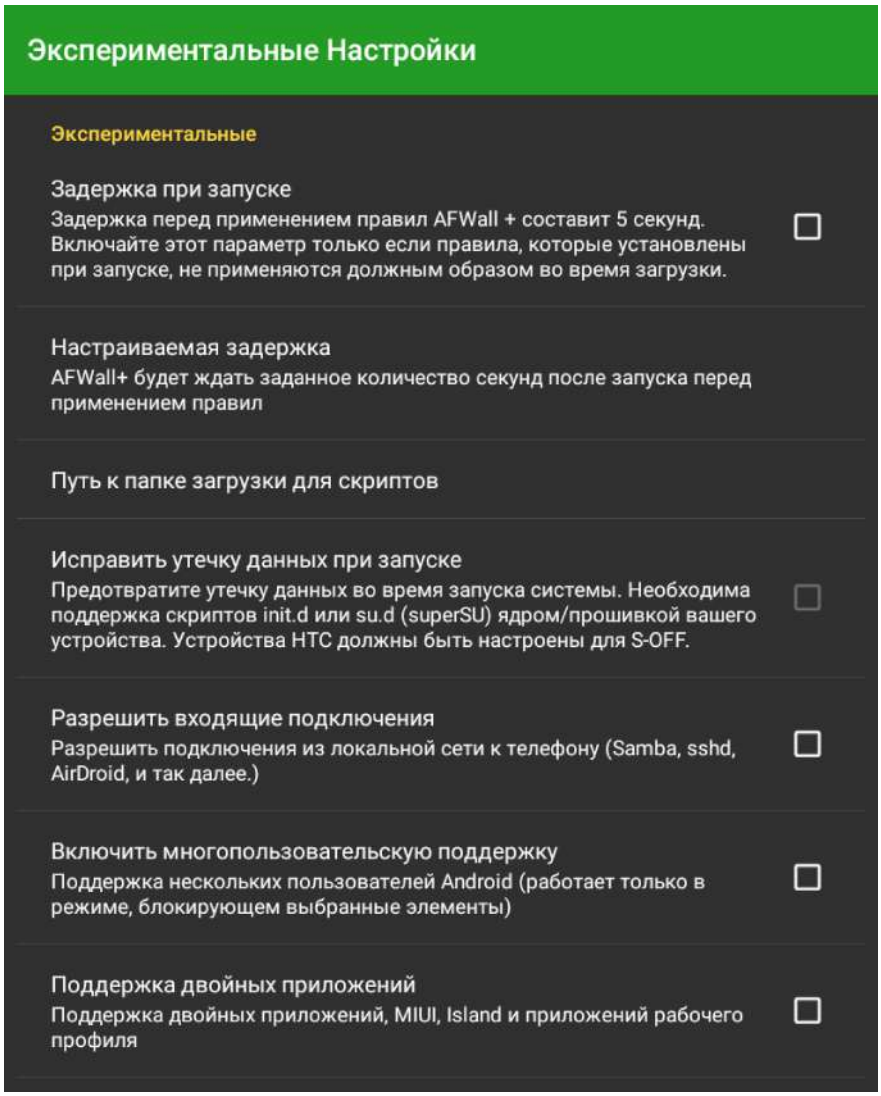


В категории «Журнал» ничего менять не нужно. Обойдемся без записей активности.

Категория «Безопасность» создана, чтобы можно было защитить доступ к приложению с помощью пароля. Эта функция может быть полезной, если вы периодически даете свое устройство кому-то попользоваться и при этом не хотите, чтобы этот кто-то поменял вам настройки файервола. Если считайте, что вам это нужно, можете ее включить. Также можете задать определенное количество попыток и включить режим невидимости на узор поля ввода.

В категории «Экспериментальные» можете задать задержку перед применением правил, если вдруг, заданные вами правила не применяются корректно. Например, вы разрешили доступ браузеру к Интернету, а он так и не может в него войти. Или вы разрешили раздачу Интернета, а она не осуществляется. Конечно, все это можно будет заметить только после задания правил. Также в этой категории можете попробовать еще что-то нужное вам, к примеру многопользовательский режим. Если у вашего устройства несколько пользователей и каждый хочет задавать свои правила файервола, то эта функция предоставляет именно такую возможность. Необходимо отметить, что иногда она работает некорректно. Крайне важной может оказаться функция «Исправить утечку данных при запуске». Дело в том, что файервол не первая программа,

которая стартует при загрузке устройства. И некоторые программы, которым мы не хотим давать доступ в сеть, при включении смартфона или планшета, могут этот доступ получить на несколько секунд, пока не запустится AFWall+. Данная функция способна предотвратить это. Однако, возможно, для этого необходимо сначала указать «Путь к папке загрузки для скриптов». И кроме того, необходим полный root, который может не иметься при стандартных настройках Magisk. В случае его получения, root нельзя будет скрыть. Лучше, конечно, перед каждой перезагрузкой/выключением, переводить устройство в режим полета, если не пользуйтесь им по-умолчанию.



Если хотите задавать несколько комплектов правил для разных ситуаций и иметь возможность быстро между этими комплектами переключаться, то такие функции настраиваются в категории «Профили». Активируйте их и настраивайте.

В категории «Бинарные» ничего менять не нужно.

В категории «Виджеты» производится настройка определенных параметров внешнего вида. Изменяйте по своему усмотрению.

В категории «Языки/плагины» можно изменить язык и отключить сообщения для плагина Tasker.

С настройкой закончили, переходим к заданию правил. В основном окне нажимаем сверху на третий значок справа и выбираем «Разрешить выбранное». Теперь все приложения, которые мы будем отмечать, будут иметь доступ в Интернет, а все остальные нет.

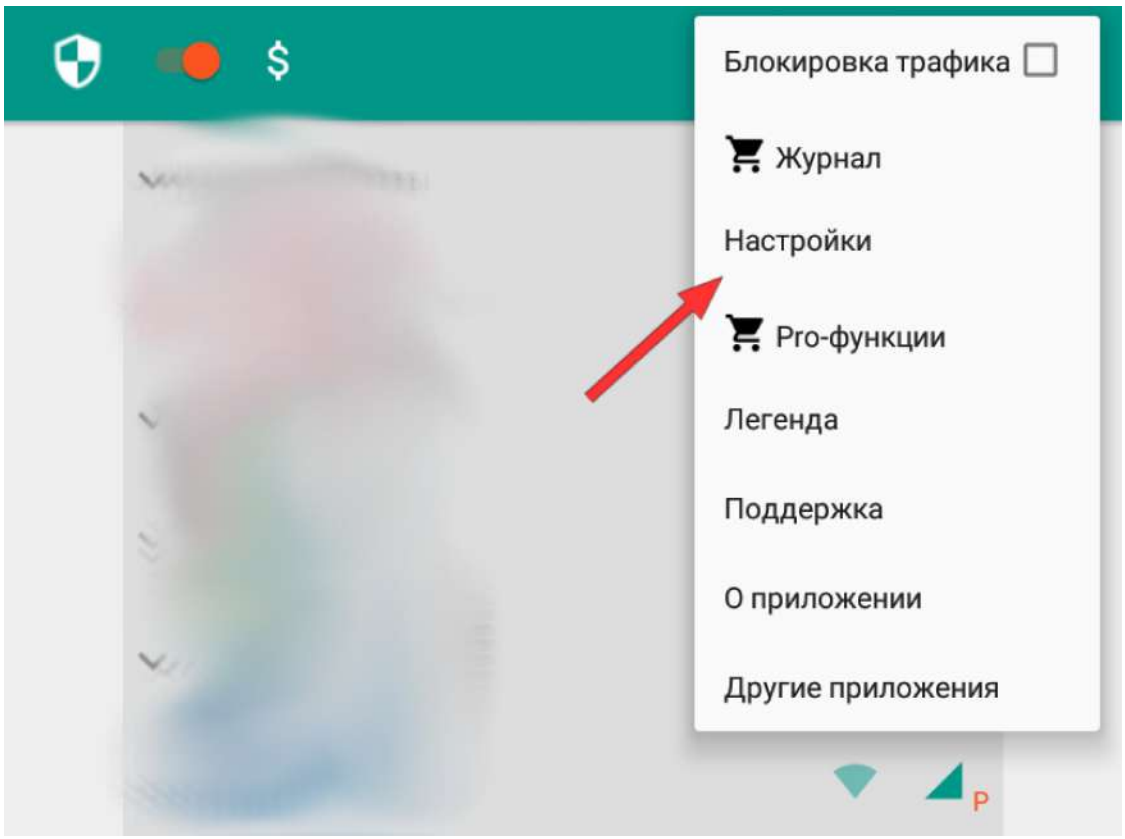
Чтобы предоставить разрешение, поставьте галочки рядом с нужным приложением, на тех способах, которыми хотите предоставлять ему Интернет. Чтобы понять какой пункт какому способу соответствует, нажмите на три точки вверху справа и смотрите «Условные обозначения». Доступ к Интернету разрешаем браузеру Icecat и F-Droid. Также, если предпочитайте синхронизировать время по Сети, разрешите (ntp) — сервера времени в Интернете. Если хотите раздавать Wi-Fi, то также разрешите (раздача) — службы DHTP+DNS. Также желательно разрешить (ядро) — ядро Linux. Без этого могут не работать некоторые функции, например отправка сообщений в свободных мессенджерах. В некоторых случаях может понадобится дать доступ (root) — приложения с root доступом. Если вы пользуйтесь геолокацией, и у вас долго определяются спутники, для решения чего вы хотите воспользоваться A-GPS,[10] можете дать доступ (gps) — GPS/GPS. Если пользуйтесь какой-то Wi-Fi сетью, где необходимо авторизовываться на специальной странице, то также необходимо активировать Captive portal login.

На этом настройка файервола пока закончена. В дальнейшем, по мере установки приложений, необходимо будет прописывать новые правила для некоторых из них.

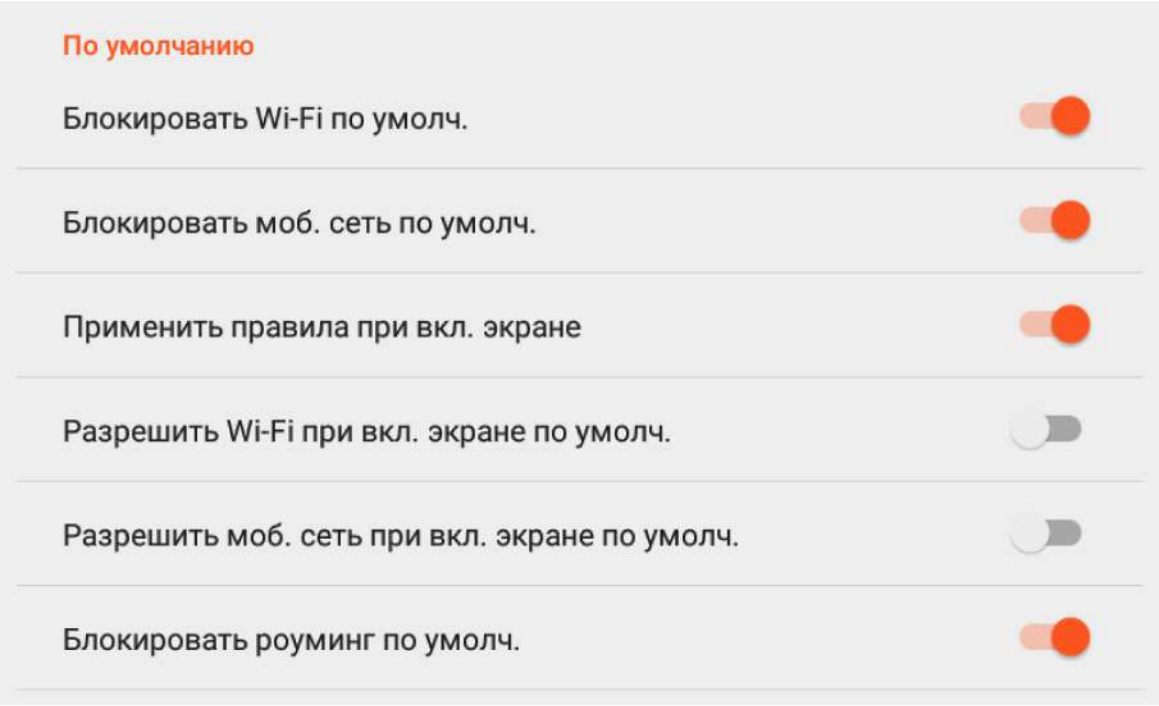
20 Установка и настройка NetGuard

Если у вас нет root-прав, то в качестве файервола можно использовать программу, создающую локальный VPN, который будет фильтровать трафик. Такой программой является NetGuard.[11] Устанавливаем его.

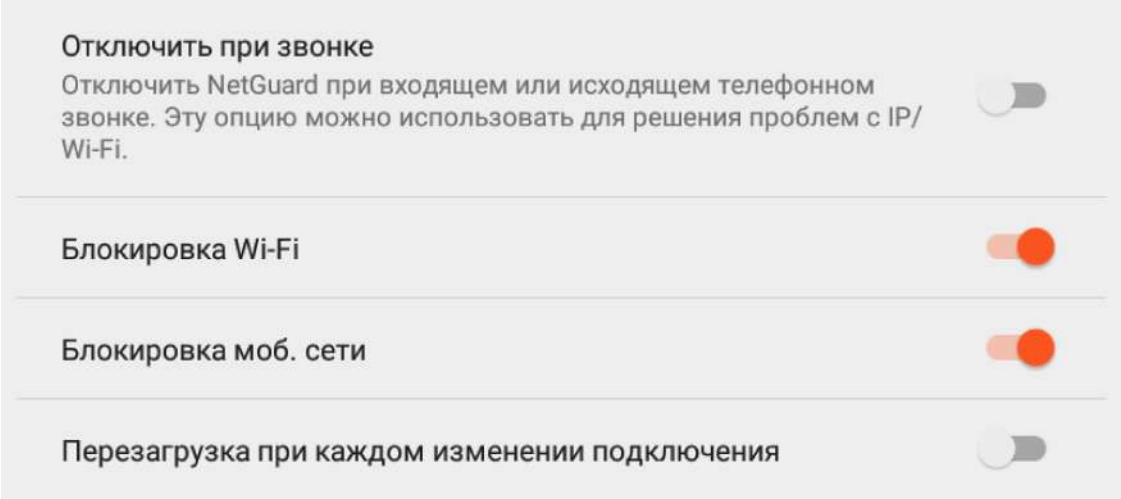
После установки запускаем и нажимаем на три точки вверху справа и выбираем «Настройки».



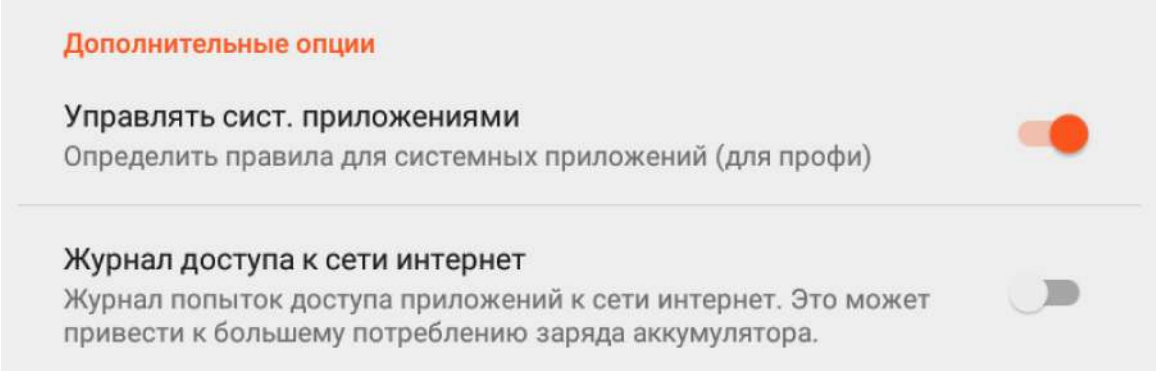
Затем выбираем «По умолчанию». Здесь активируем «Блокировать Wi-Fi по умолчанию», «Блокировать моб. сеть по умолчанию», «Применить правила при вкл. экрана» и «Блокировать роуминг по умолчанию».



Возвращаемся в настройки и выбираем «Параметры сети». Здесь листаем вниз и проверяем, чтобы были активны «Блокировка Wi-Fi» и «Блокировка моб. Сети».



Возвращаемся в настройки и выбираем «Дополнительные опции». Активируем «Управлять сист. Приложениями».



После этого возвращаемся в основное окно программы и включаем ее, нажав на ползунок вверху слева. При этом выскочит сообщение о том, что приложение пытается настроить соединение VPN. Разрешаем ему это. Затем активируем доступ к сети только у тех приложений, которым это действительно нужно. В нашем случае это пока только F-Droid и браузер IceCat Mobile. Для активации нажмите на перечеркнутые оранжевые значки Wi-Fi и мобильного Интернета справа от значков и названий приложений. Значки станут зелеными. После этого закрываем окно. Приложение будет работать в фоне. Таким образом будет предотвращен слив информации несвободными приложениями.

Если данная программа откажется работать на вашем устройстве, альтернативой ей может стать приложение Blokada.[12] Оно также создает локальный VPN и через него фильтрует трафик. Также позволяет предотвратить проникновение на устройство по определенным протоколам.

21 Установка основных приложений

Все приложения первостепенной важности представлены серией Simple Mobile Tools, имеющей характерные оранжевые значки.[13]

В качестве галереи подойдет приложение Simple Gallery.[14] Содержит все основные функции для просмотра изображений и видео. Имеет самые простые функции редактирования. Есть ее старая версия отдельным приложением, нужна новая (версии от 6 и выше). Если данное приложение будет работать некорректно или по каким-то другим причинам не устроит вас, в качестве альтернативы можно порекомендовать приложение Camera Roll.[15]

Для камеры подойдет приложение Simple Camera.[16] Также имеет все, что нужно для создания фотографий и видео. Если данная программа вам не подходит, можете попробовать Open Camera.[17] Это более функциональный инструмент.

В качестве календаря можете использовать Simple Calendar.[18] Содержит все необходимые такой программе функции. Создание заметок разной маркировки, создание маркировок, настройка оповещений и т.д. Есть его старая версия отдельным приложением, нужна новая (версии от 6 и выше).

В качестве файлового менеджера подойдет Simple File Manager.[19] Данная программа может попросить root-права. Если не знайте для чего конкретно можете их использовать, не предоставляйте. Есть его старая версия отдельным приложением, нужна новая (версии от 6 и выше). К сожалению, на некоторых устройствах, через него плохо работает передача файлов по Bluetooth. Поэтому альтернатива ему Dir.[20]

Если на устройстве имеется фонарик, то для его использования можете установить программу Simple Flashlight.[21] Данная программа содержит различные режимы работы фонарика.

В качестве аудиоплеера подойдет программа Simple Music Player.[22] Позволяет прослушивать музыку и аудиозаписи, создавать плейлисты. Как и большинство таких программ, может работать в фоне. Если не устраивает,

можете попробовать программу Vanilla Music.[1] К ней имеется также несколько дополнений для различных функций, к примеру контроля метаданных.

Если хотите что-нибудь простенькое для рисования, подойдет инструмент Simple Draw.[2] Несколько более продвинуто выглядит программа Markers.[3]

В качестве калькулятора можете использовать Simple Calculator.[4]

В качестве часов прекрасно подойдет программа Simple Clock.[5] Помимо отображения времени и даты, в функциях также имеется будильник, таймер и секундомер. Если нужен крупный виджет времени и даты, могу порекомендовать Fairphone Clock Widget.[6]

В качестве диктофона подойдет Simple Voice Recorder.[7] В качестве более функциональной альтернативы можно посоветовать Audio Recorder.[8] Если же нужен диктофон, способный записывать звонки, подойдет программа Call Recorder for Android.[9] Есть как более старая, так и более новая версии. Более свежая не требует доступа к Интернету.

В качестве приложения для совершения звонков и просмотра вызовов подойдет программа Simple Dialer.[10]

Если нужно безопасное приложение для контактов, используйте Simple Contacts.[11] Есть его старая версия в отдельном приложении, нужна новая (версии от 6 и выше).

Для SMS есть программа Simple SMS Messenger.[12]

В линейке этих простых приложений есть и программа для создания заметок Simple Notes.[13] Однако мне она показалась неудобной. Более подходящим на мой взгляд будет приложение Editor,[14] а в качестве альтернативы можно назвать SNotepad.[15]

Что ж, теперь на вашем устройстве есть все самое необходимое. Конечно, этим функционал современного смартфона и планшета не ограничивается, поэтому далее я расскажу о приложениях для самой разнообразной деятельности.

Для воспроизведения видео, как я уже говорил, можно использовать обычную Галерею. Но она не всегда может воспроизвести файл. Для просмотра любого видео подойдет мобильная версия VLC.[16] Данный проигрыватель читает все форматы видео и аудио, позволяет составлять библиотеку,

распределяя файлы по категориям. Видео, у которых названия начинаются одними словами, помещаются в отдельную категорию. Очень удобное приложение.

С просмотром офисных документов неплохо справляется программа LibreOffice.[17] Хотя и не всегда ей удается открыть документ корректно. Позволяет открывать текстовые файлы, электронные таблицы и презентации форматов как ODF (odt, odc, odp), так и MS Office (doc, docx, xls, xlsx, ppt, pptx).

Для чтения электронных книг и PDF-файлов подойдет программа Librera Reader.[18] Имеет удобный интерфейс и располагает большим количеством функций. Читает большое количество форматов, в том числе fb2, pdf, djvu, epub. Альтернативой может стать программа MuPDF mini.[19]

Для сканирования QR-кодов и штрих-кодов можно использовать Сканер штрих-кодов Barcode Scanner.[20] Будучи подключенным к Интернету может искать информацию о продуктах, такую как цены и отзывы. Для этого, понятное дело, этой программе нужно дать доступ к Интернету в файерволе. Альтернативами являются «Сканер QR и штрихкодов»[1] и Binary Eye.[2] Если желайте только сканирование QR-кодов, и чтобы программа не имела даже потенциальной возможности доступа к Интернету, подойдет QR Scanner.[3]

В качестве мощного инженерного калькулятора подойдет программа WhatExp.[4] Помимо самих расчетов позволяет строить графики.

В качестве матричного калькулятора подойдет Matrix Calc.[5] Позволяет производить расчеты с матрицами форматов 2x2, 3x3 и 4x4.

Для отслеживания процессов на устройстве и затраченных ресурсов можно порекомендовать AnotherMonitor.[6]

Для записи видео с экрана смартфона или планшета подойдет программа ScreenCam.[7] В программе можно настраивать параметры записываемого видео, такие как разрешение, частота кадров и битрейд. Также можно установить во время записи включение микрофона. А также включение камеры, как основной так и фронтальной, которые можно менять прямо во время записи. По умолчанию запись с камер будет отображаться на экране в виде небольшого окошка, которое можно при желании развернуть на весь экран.

Для распаковки zip-архивов подойдет программа Squeez.[8]

В качестве оффлайн-словаря можно использовать DictionaryForMIDs.[9] После установки программы в нее нужно импортировать сами словари, которые можно скачать отдельно и добавить из файла или скачать непосредственно с помощью этой программы. Для этого ей нужно будет предоставить доступ к Интернету, в файерволе. После скачивания нужных словарей, это разрешение можно будет убрать.

Если необходимо конвертировать видео, можно использовать программу Video Transcoder.[10] К сожалению, не всегда в состоянии осилить крупные файлы.

Для чистки устройства от мусора, временных файлов можно использовать приложение LTE Cleaner.[11] Оно не копается в глубине многих отдельных приложений и поэтому не может вычистить ваше устройства слишком тщательно. Однако, все же удаляет много шелухи, скапливающейся на устройстве по мере эксплуатации.

Если опасаетесь подслушивания через какие-то приложения, или залетевший вирус, то для его предотвращения можно воспользоваться приложением PilferShush Jammer.[12] Оно программно блокирует микрофон, тем самым лишая несвободные инструменты возможности вести прослушку. Существует два режима подавления микрофона. Один пассивный, это собственно, блокирование микрофона. Другой активный, когда микрофон не блокируется, а просто зашумляется. Такой вариант менее надежен, к тому же устройство начинает громко издавать звуки, и я его не рекомендую. К сожалению, это приложение нещадно расходует заряд батареи, поэтому пользоваться им на постоянной основе вряд ли хорошая идея. Тем не менее в отдельных ситуациях, оно может пригодится.

Для шифрования текста можно использовать приложение SimpleTextCrypt [13] . В качестве альтернативы можно обратить внимание на Encrypt Text.[14]

Для создания зашифрованных заметок подойдет приложение Note Crypt Pro.[15] Если данное приложение вас не устраивает, можете попробовать альтернативу, SealNote.[16]

Если вам необходимо приложение для создания зашифрованных контейнеров, в которые можно было бы поместить что угодно, то вам поможет программа EDS Lite.[17]

Приложением для шифрования с широким набором функционала является OpenKeychain.[18] С помощью нее можно создавать ключи шифрования, зашифровывать и расшифровывать текст и файлы, а также производить шифрование OpenPGP в различных приложениях, например шифровать почту в K9 Mail или канал общения через XMPP в Conversation.

Для внедрения шифрования в любой вводимый на экране текст существует программа Oversec.[19]

В F-Droid большое количество приложений для различной научной деятельности. Из простых примеров можно привести приложение Elementary,[20] представляющее собой Периодическую таблицу химических элементов, где про каждый элемент имеется основная информация. Есть и куда более специфические программы. Например, Calcvac,[21] вычисление логарифмических одномерных профилей давления в вакуумных трубах. Есть приложения для различного интерактивного обучения, в том числе языкам.

Этичных приложений для самых разных задач масса. Конечно, здесь я представил далеко не все. Далее я расскажу о приложениях для различной Интернет-активности и обеспечения безопасности.

22 Мобильные браузеры и почта

Как и в случае с компьютером, иногда полезно иметь несколько браузеров для разной активности. Некоторые можно установить из уже известного приложения FFUpdater. Firefox Бета-версия и Firefox Night, это тестовые версии, поэтому их я рекомендую не трогать. Firefox Focus имеет неплохие настройки безопасности, но к сожалению, не позволяет устанавливать расширения. Кроме того, в нем нет возможности работы с несколькими вкладками. Все тоже самое относится к Firefox Klar.

Браузер Brave, несмотря на то, что он имеет репутацию защищенного браузера и действительно обладает гибкими настройками безопасности, а также возможностью гулять в сети Tor, я не рекомендую. В прошлом в нем присутствовал функционал подставления реферальных ссылок на майнеры и криптокошельки, который осуществлялся, когда пользователь проходил на те или иные ресурсы.[22] Разработчики объяснили причину этой проблемы и убрали ее.[1] В дальнейшем выяснилось, что в нем присутствуют также DNS-утечки при обращении пользователей к ресурсам onion-пространства.[2] Эту

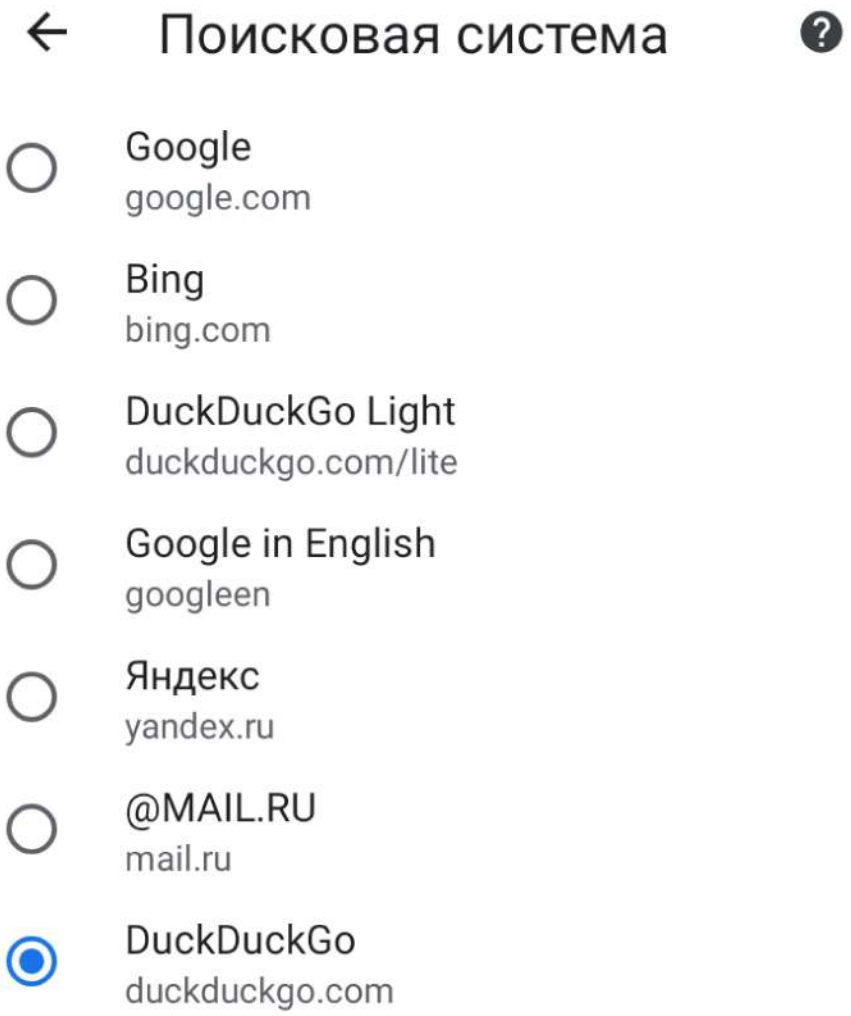
проблему также устранили. Также известно, что данный браузер сливает информацию на ресурсы, торгующие пользовательскими данными.[3] Убран ли этот функционал, мне найти информацию не удалось. Помимо этого в нем не блокируются трекеры от Facebook и Twitter. Разработчики отказываются устранять эту проблему, заявляя, что это, якобы необходимо для функционирования многих сайтов.[4] Это не так. Не считая сайтов самих Facebook и Twitter, чрезвычайно редкие ресурсы отказываются корректно работать без исполнения их скриптов. Подобное разрешение шпионить за пользователями неприемлемо. Все это не позволяет считать браузер Brave приемлемым для использования.

Что касается классического Firefox, то он хорошо подойдет как дополнительный браузер. В нем не самые гибкие, но все же ощутимые настройки безопасности. Если с ними не усердствовать, то он будет открывать корректно сайты, которые не будут открываться в Iceraven.

Если у вас планшет и вы хотите, чтобы вкладки отображались подобно тому, как в браузерах на компьютере, если вы прежде пользовались, например, браузером IceCat, ныне не поддерживающемся, то для вас наилучшим вариантом будет браузер Bromite. Он имеет достаточно гибкие настройки безопасности. Есть встроенная блокировка рекламы. К сожалению, в него

невозможно установить расширения. В отличии от других предлагаемых браузеров, он основан на Chromium, соответственно, подойдет и тем, кому нужен браузер, подобный Chromium (некоторые ресурсы позволяют работать с собой только через такие браузеры). Как дополнительный браузер он подойдет идеально.

После установки, запускаем его, нажимаем на три точки справа сверху и идем в «Настройки». В категории «Поисковая система» выбираем DuckDuckGo. К сожалению, нет возможности удалять предустановленные поисковые плагины, но выбрав DuckDuckGo, на остальные можно просто не обращать внимания.



Запоминание паролей и способов оплаты по-умолчанию отключены. В категории «Адреса и другие данные» я рекомендую отключить автоматическое подставление адресов.

В категории «Конфиденциальность и безопасность» изначально выставлены хорошие настройки приватности. Нажимаем на «Использовать безопасный DNS-сервер». Обычно используются DNS-сервера провайдера, и через них запросы идут в незашифрованном виде. Это создает возможности для сторонних наблюдателей подсмотреть эти запросы, а значит узнать, какие ресурсы вы посещаете. А также позволяет подменять передаваемые данные, в результате чего вы можете попасть на поддельный ресурс. Ввиду этого целесообразно использовать шифрованные DNS. В данном браузере он по-умолчанию включен, но при этом используется сервер от крупной корпорации Cloudflare. Ей лучше предпочесть что-то другое. Нажимаем «Выбрать другого поставщика», выбираем «Персонализированные» и в поле «URL поставщика» указываем адрес DNS-сервера, поддерживающего технологию шифрования. Такие сервисы можно посмотреть на странице проекта DNSCrypt.[5] Из представленных сервисов можно выбрать любой, у которого указан протокол DoH. Главное, чтобы это не была крупная корпорация, вроде Google и Cloudflare. Также желательно, чтобы он не вел логирование и цензуру (был помечен как non-logging и т.п.), а также, чтобы поддерживал технологию DNSSEC. Она предназначена для проверки подлинности DNS-запросов, что предотвращает их подмену. Если у вас вдруг возникнут сложности с выбором, то можно в крайнем случае вместо «Персонализированные» указать «OpenDNS». Это, в принципе, неплохой сервис. На этом настройка данного параметра закончена. Также я рекомендую отключить «Заполнять поисковые запросы и URL автоматически».

В категории «Настройки сайтов» проверьте, чтобы были заблокированы геоданные, камера, микрофон, датчики движения, всплывающие окна и

переадресация, реклама, фоновая синхронизация. Также заблокируйте защищенный контент, устройства с NFC, USB, буфер обмена. Еще следует отключить функции в разделах — «Виртуальная реальность», «Дополнительная реальность», «Использование устройства». В разделе «Файлы cookie» лучше поставить «Блокировать сторонние файлы cookie». Однако, поскольку некоторые сайты могут перестать открываться, а браузер нужен именно для открытия таких ресурсов, то можете оставить «Разрешать файлы cookie».

В категории «User Agent» есть возможность подмены типа браузера и операционной системы. Однако в этой функции нет предустановленных типов подмены, их необходимо вводить вручную, что проблематично для неподготовленного пользователя.

На этом настройка браузера Bromite закончена.

К сожалению, разработка Bromite идет крайне медленно, и вполне может создастся ситуация, в которой некоторые сайты перестанут корректно открываться. В этом случае, в качестве варианта, пожалуй, стоит рассмотреть браузер Vivaldi. Его дизайн заметно отличается от классического Chromium, в том числе у него расположение вкладок подобно Bromite.[6] Основная функциональная часть браузера во многом идентична Chromium, хотя некоторые отличия имеются.[7] Стоит отметить, что разработчики предприняли некоторые меры по противодействию слежки Google,[8] из-за чего эта корпорация пыталась даже препятствовать распространению Vivaldi.[9] Функциональная часть браузера, как и Chromium, с которого она взята, находится под свободной лицензией. А вот оформление не является свободным. Таким образом, Vivaldi не является полноценно свободным браузером. Однако, при этом все оформление написано на обычном HTML и CSS, и к его тексту можно получить доступ. То есть, хотя вы не имеете права копаться в исходном коде данных компонентов браузера, вы фактически можете это делать. Сами разработчики Vivaldi заявляют, что не осуществляют преследование пользователей за такие действия. Единственное против чего они выступают категорически против, это чтобы данный их код использовался в коммерческих целях. Если свести всю их аргументацию к одной фразе — они так борются с конкуренцией.[10] Этот момент не очень понятный, — если они не хотели только чтобы их код использовали в коммерческих целях, то почему использовали лицензию, запрещающую вообще какой-либо доступ к исходному коду? Почему не взяли ту, которая просто налагает ограничения на

коммерческое использование? Этот момент совершенно не понятный. Также необходимо отметить, что Vivaldi собирает некоторые пользовательские данные. При его установке создается id конкретной установленной копии, и каждые сутки на сервера разработчиков отсылается информация, помеченная этим id, об архитектуре системы, времени последнего сообщения с сервером и ip-адрес. У ip удаляется последний октет, что не позволяет установить, кому конкретно он принадлежит, а можно узнать лишь страну, в которой пользователь производит подключение. Никакая другая информация не собирается.[11] Несмотря на это данный браузер все же более приглядный, чем классический Chromium, он собирает меньше информации.

Все другие браузеры, распространяемые через данное приложение, очень специфические либо недостаточно корректно работающие. Это относится, в том числе, и к Ungoogled Chromium.

Непосредственно в F-Droid обратить внимание можно разве что на Privacy Browser.[12] В нем весьма серьезные настройки безопасности, есть возможность быстрого блокирования java-скриптов, cookie-файлов, рекламы, трекеров. Есть возможность подмены типа браузера и ОС. К сожалению, в нем отсутствует возможность гибкой работы со скриптами, а установить для этого noscript нельзя. В общем-то, это единственная причина по которой я не могу рекомендовать его в качестве основного браузера. Также возможно взаимодействие с приложением Orbot, о котором я расскажу далее, для пропускания трафика через Tor. Однако использовать его для приватной активности сомнительная идея, поскольку в нем включен WebRTC и нет возможности его отключения. А посему, ваш ip будет слит. Тем не менее, просто как дополнительный полнофункциональный браузер, Privacy Browser вполне подходит.

В качестве же почтового клиента, посоветовать можно K9 Mail.[13] Очень удобный клиент. Позволяет добавлять в себя несколько почтовых ящиков, естественно, распределять в них письма по папкам. Хранить письма позволяет непосредственно на устройстве, а также присутствует функция создания зашифрованных писем. Последняя, как я уже подчеркивал, для публичной почты весьма сомнительна, но может кому и будет необходима. В качестве альтернативы можно назвать клиенты FairEmail[14] и SimpleEmail.[15] Если вам все же нужны клиенты с упором на шифрование и защищенность, то также можно указать Pretty Easy Privacy[16] и Delta Chat.[17] Также, если хотите

использовать защищенную почту Tutanota, в F-Droid есть отдельный клиент для нее.[18]

23 Работа с KeePass DX

Разумеется нам не обойтись без менеджера паролей. Одним из наиболее удобных таких программ для Android является KeePass DX.[19] Его функционал почти полностью идентичен функционалу KeePass2. Также как и он, эта программа, хранит базу паролей на устройстве в зашифрованном виде, удаляет логины и пароли из буфера обмена по прошествии определенного времени после их копирования туда. В ней можно генерировать пароли заданной длины и выбирать, какие типы символов он будет содержать. Все пароли распределяются по категориям и подкатегориям, с привязкой к логинам и названиям ресурсов. В общем в программе есть все необходимое. Устанавливаем ее.

Данная программа работает с тем же форматом файлов баз паролей, что и KeePass2, поэтому вы можете просто скопировать уже имеющуюся базу паролей на устройство. Для того, чтобы открыть ее, нажмите в главном окне кнопку «Выбрать существующую базу паролей» и выберите файл в той папке, где он лежит.

Также вы можете создать новую базу паролей, нажав в главном окне «Создать файл KeePass». В появившемся окне выберите путь, где будет храниться файл с базой паролей и название. Далее введите дважды пароль. Я рекомендую, чтобы не путаться использовать тот же пароль, который вы задали для разблокировки устройства. У поля «Файл ключа» можно снять галочку. Хотя если хотите, вы можете использовать эту функцию.

В появившейся базе, нажав на кнопку плюс (+) внизу справа вы можете добавить категорию, нажав «Новая группа» или новую запись с паролем, нажав «Новая запись». Внутри категорий также можно создавать подкатегории или непосредственно записи с паролями.

Для создания категории вам нужно ввести только название. Для создания записи с паролем нужно ввести название, логин и, собственно, пароль, подтвердив его. Если нажать на знак ключа рядом с полями для ввода пароля, то можно сгенерировать пароль. В появившемся окне можно выбрать длину пароля и то, какие типы символов он будет содержать. После изменения количества символов и отметки новых галочек, либо снятия старых, нужно

нажать на кнопку «Генерация пароля». Новый пароль будет сгенерирован и для его утверждения необходимо лишь нажать кнопку «Принять» внизу справа. Также здесь можно указать ссылку и добавить комментарий. Еще можно добавить дополнительные параметры записи. Для этого нужно нажать знак плюс (+) внизу слева. После чего нужно ввести название поля и его значение.

Вот в принципе и все что нужно для использования этой программы. Конечно, у нее еще много других настроек, но это уже для более искушенных пользователей. Если по каким-либо причинам данная программа вам не подойдет, альтернативой может стать KeePass Droid.[20] Функционал очень схож.

24 Инструменты навигации

В F-Droid довольно много приложений для просмотра карт и прокладки маршрутов. Некоторые из них позволяют также искать определенные места и узнавать о них информацию из Интернета.

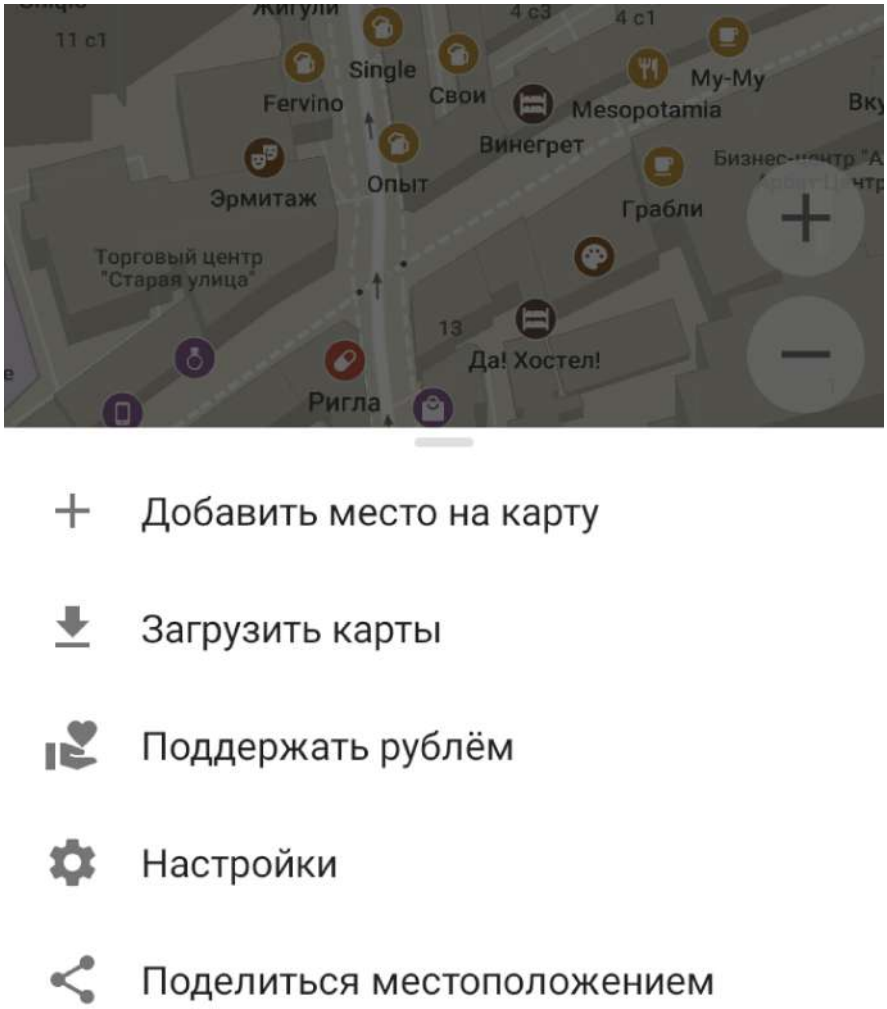
Первым для рекомендации является приложение Organic Maps.[21] Как и все другие этичные программы карт и навигации, использует свободный сервис OpenStreetMap. Основным достоинством данного приложения является оффлайн-навигация. То есть просмотр карт осуществляется не путем обращения к серверу, а непосредственно на устройстве. То есть, карты можно смотреть, искать адреса и прокладывать маршруты будучи отключенным от Сети.

После установки в файерволе предоставляем ему доступ к Интернету. В дальнейшем, если захотите, можете это разрешение убрать и предоставлять снова только для обновления карт. А пока карты еще нужно скачать.

При открытии приложение сообщит, что необходимо скачать общую карту мира. Соглашаемся. Затем можно будет скачать карты непосредственно тех регионов, которые вам нужны. Вы конечно можете скачать карты всех уголков мира, но весить это будет ни один гигабайт. Для скачивания просто приблизьте, растягиванием карты тот город или область, для которой вы хотите получить карту. В определенный момент выскочит предложение скачать карту для данного региона. Скачивайте то, что вам нужно. Также, если у вас отключены геоданные, может выскочить предложение включить геолокацию. Тут уже на ваш выбор.

Итак, перед нами загруженное приложение для просмотра карт, поиска тех или иных мест, прокладки маршрутов и навигации. Карты представляют собой стандартные карты OpenStreetMap.

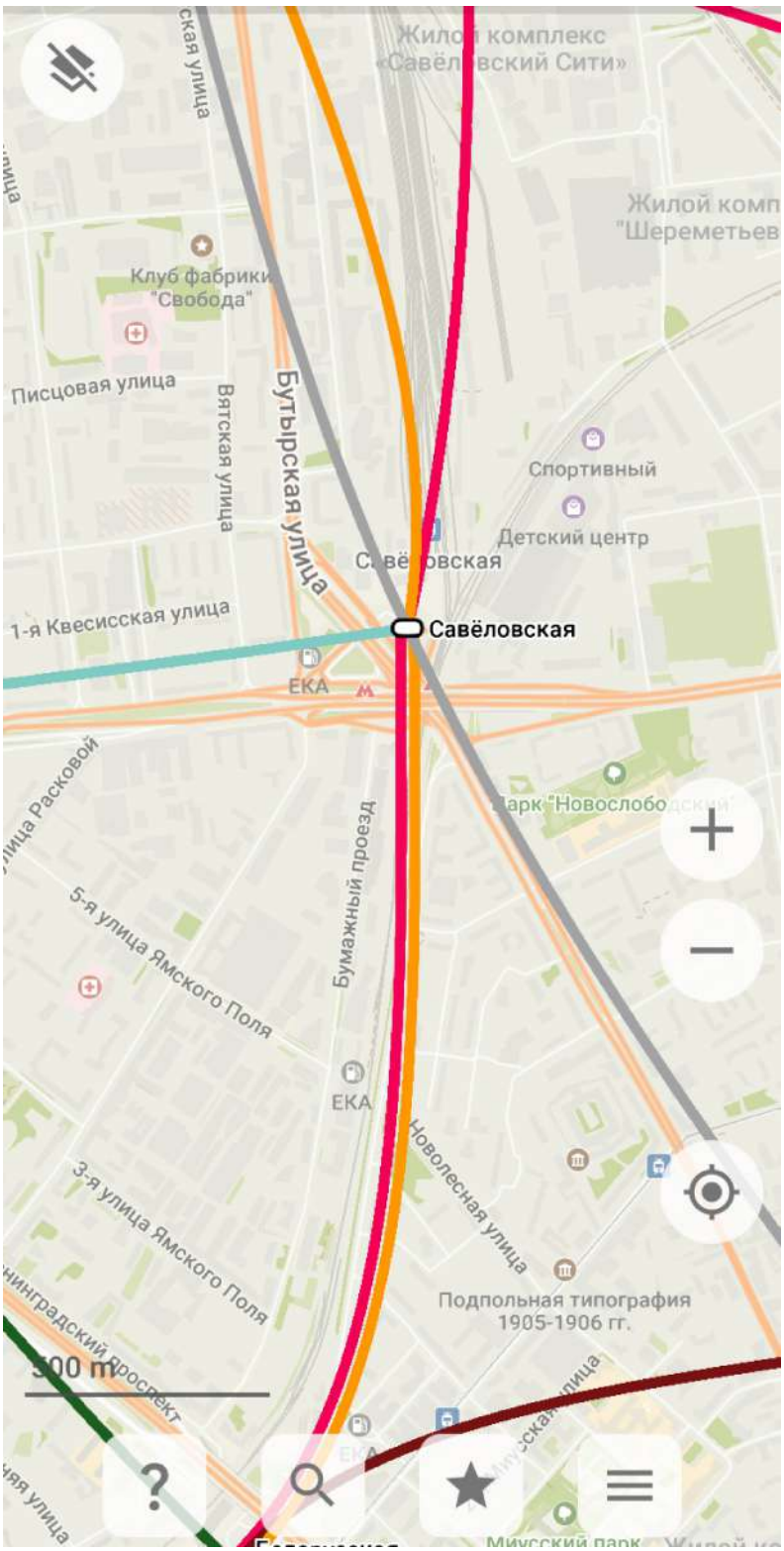
Нажав на три черты внизу справа мы увидим функции добавления мест на карту, загрузке карт, а также настройкам.



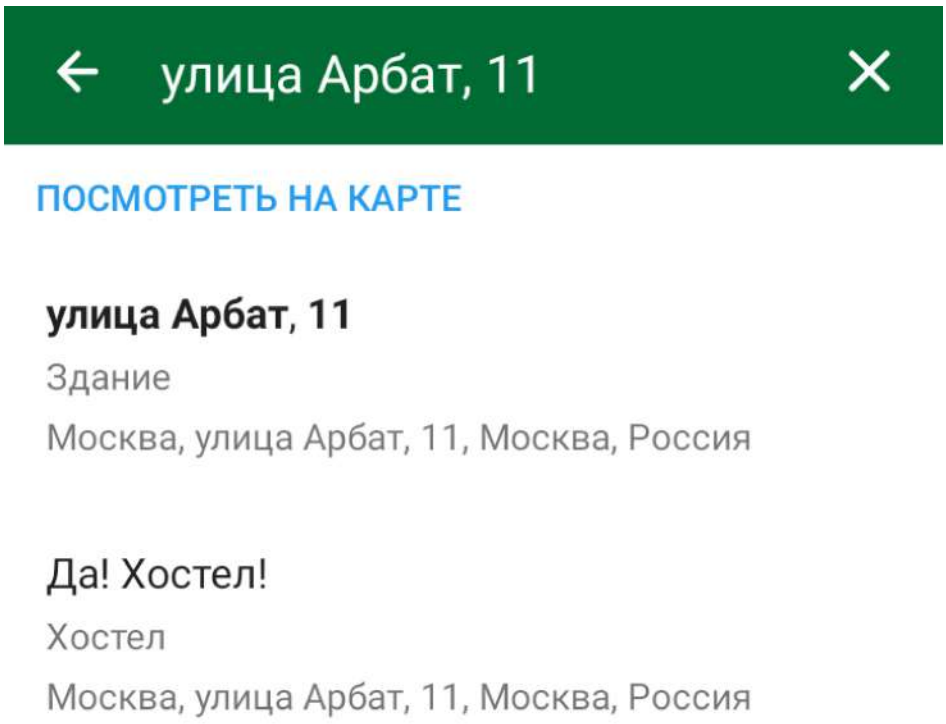
Если пройти в них, то можно настроить внешний вид приложения, включить энергосбережение, включить доступ к информации из Интернета для отображения деталей, таких как фотографии и отзывы о заведениях. Также можно включить голосовые инструкции.

В приложении также присутствует возможность делиться своим местоположением отправляя данную информацию через ресурсы коммуникации.

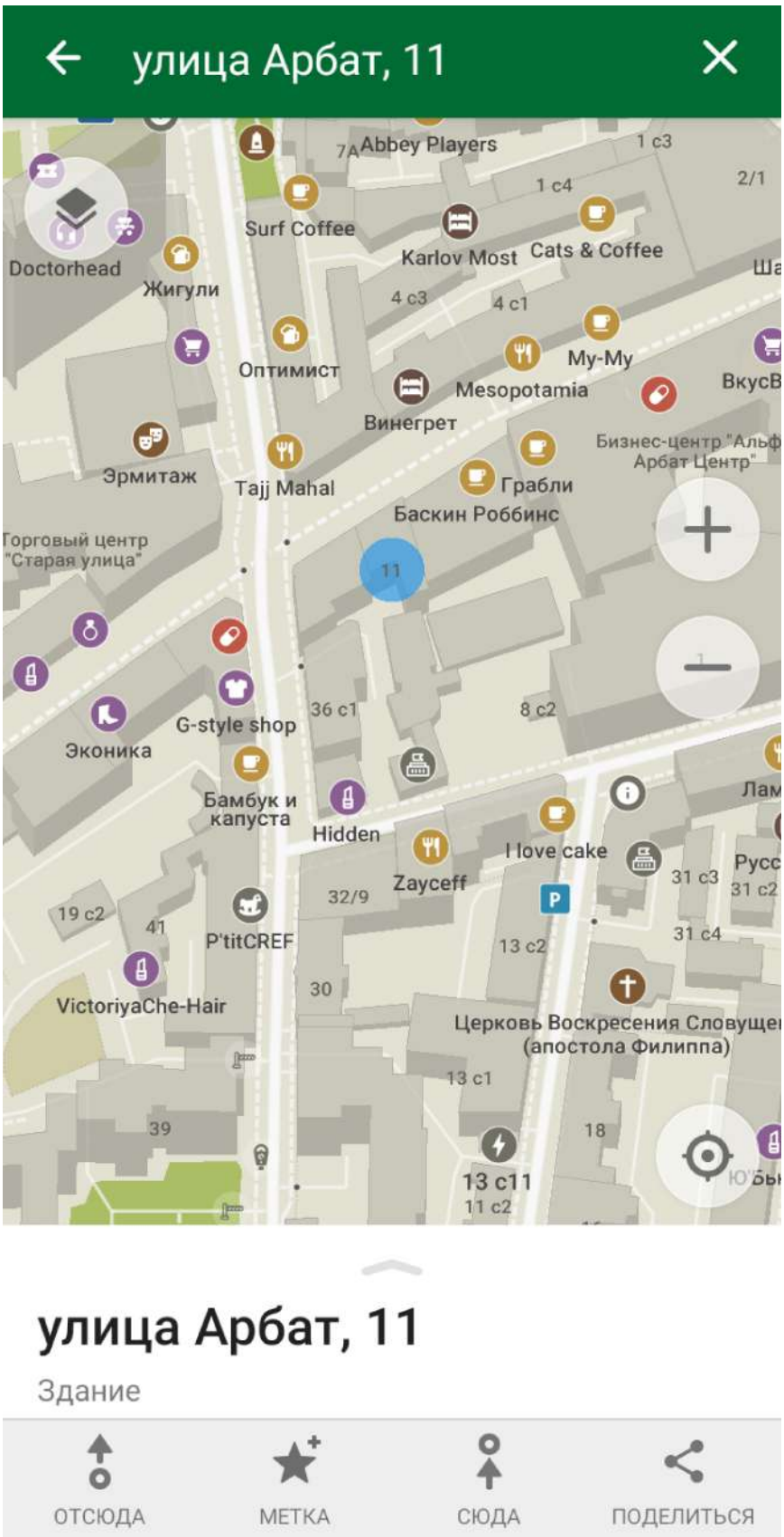
Если в окне карт нажать на значок слева сверху, то можно включить отображение слоев карты, например высот или линий метро.



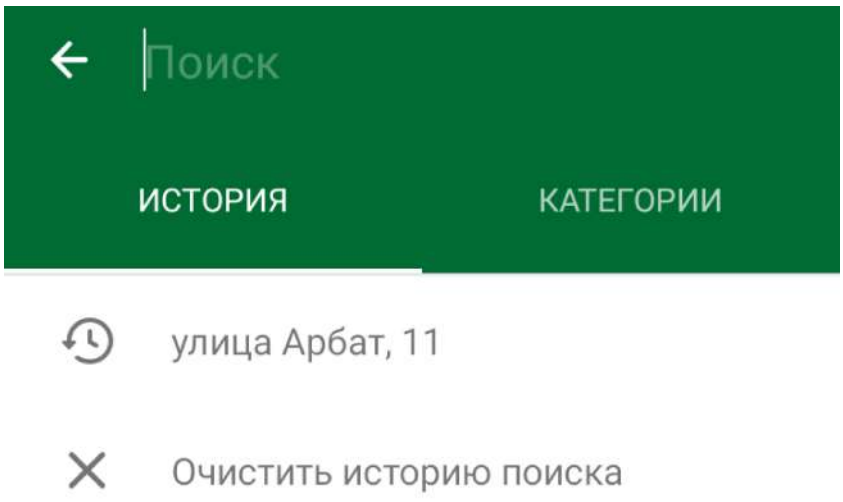
Значок лупы внизу активирует функцию поиска адресов. Для того, чтобы найти на карте какой-нибудь адрес, наберите в строке поиска этот адрес, и программа выдаст вам варианты.



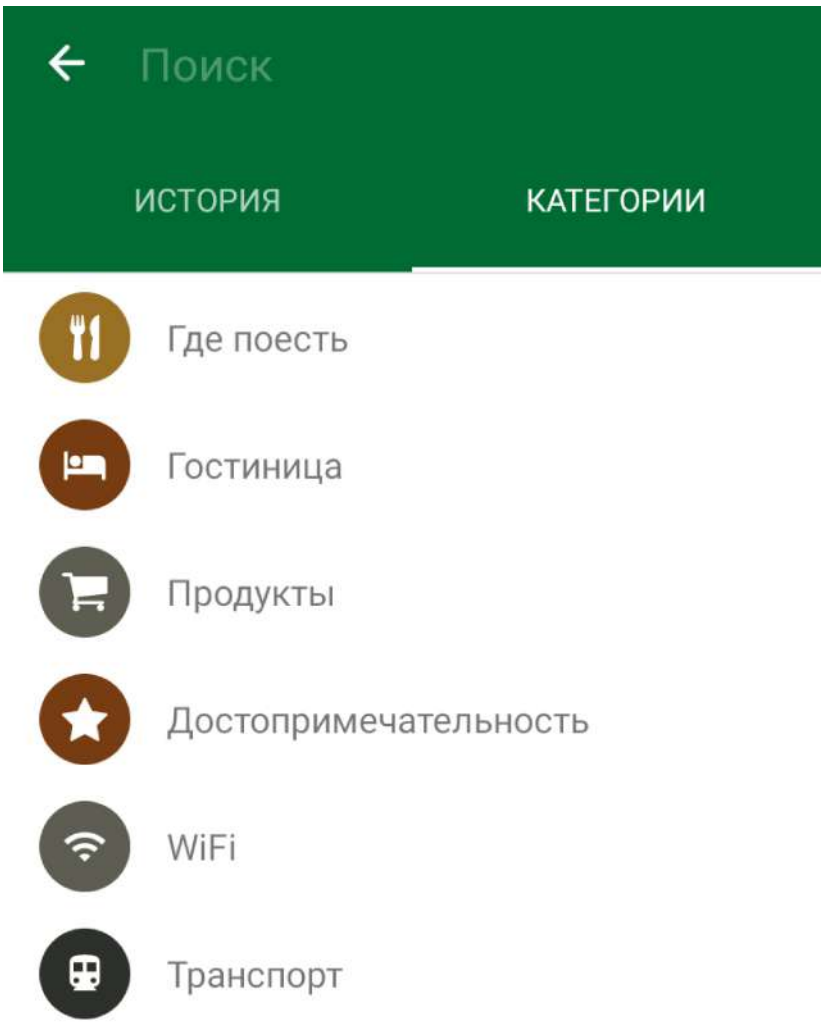
После чего выберите один из этих вариантов, нажав на него, и этот адрес откроется на карте и будет отмечен.



Во вкладке «История» отображаются те адреса, которые вы уже искали.



Во вкладке «Категории» отображаются типы мест, такие как гостиницы, магазины, достопримечательности, общие точки доступа Wi-Fi и т.д.



Если нажать на одну из категорий, отобразится список соответствующих мест по адресам.

ПОСМОТРЕТЬ НА КАРТЕ

Хлеб Насущный
Булочная
Москва, улица Арбат, 6/2, Москва, Россия

Tajj Mahal
Ресторан • Индийская кухня
Москва, улица Арбат, 6/2, Москва, Россия

Krispy Kreme
Кафе • Пончики
Москва, улица Арбат, 6/2, Москва, Россия

Вуле-Ву Закрыто
Ресторан
Москва, улица Арбат, 9, Москва, Россия

Фабрика плова
Кафе
Москва, улица Арбат, 10, Москва, Россия

Пельмени да борщи
Ресторан
Москва, улица Арбат, 10, Москва, Россия

После нажатия на который, это место откроется на карте.

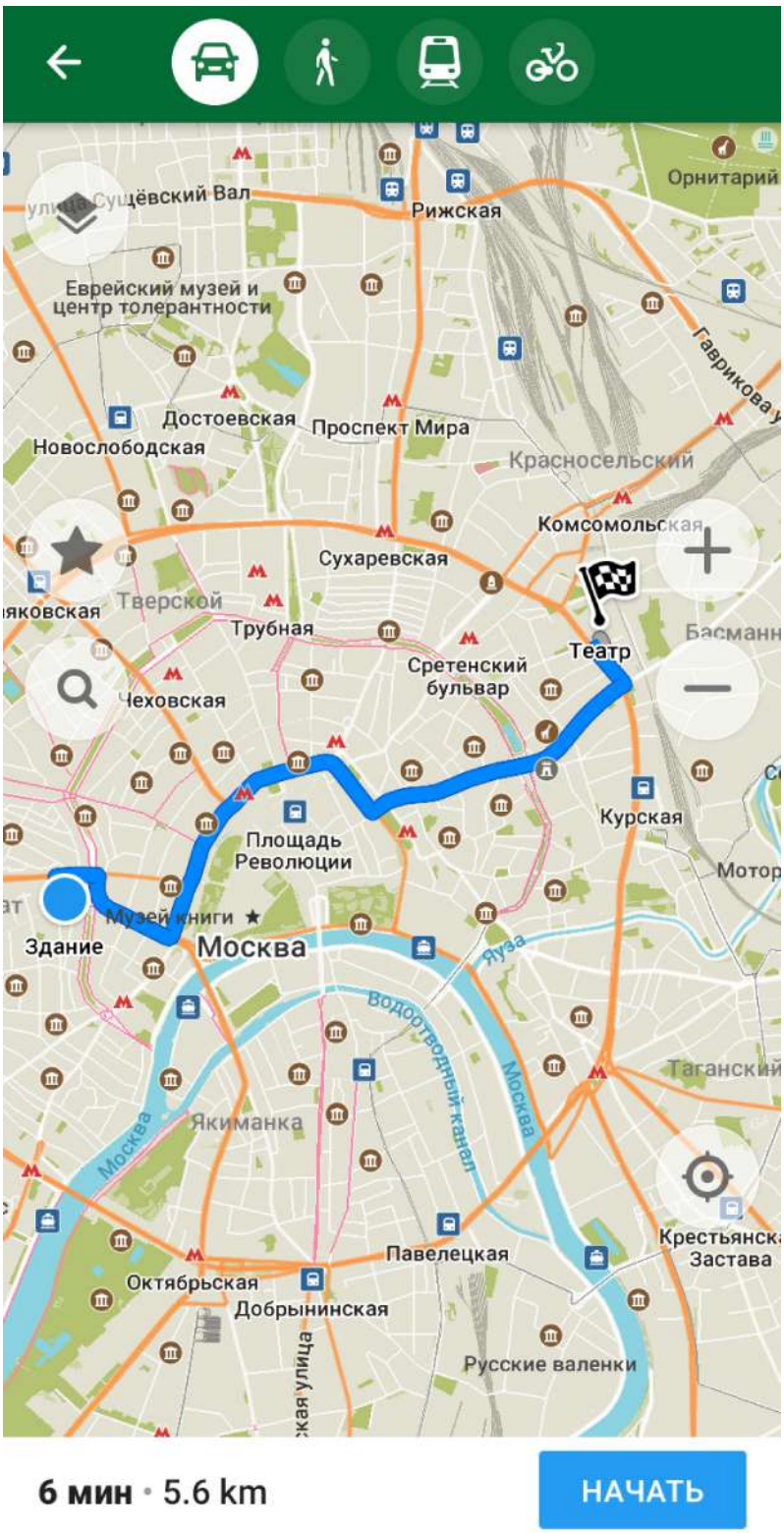
В окне карт первый значок внизу слева — прокладка маршрута. При нажатии на него, сверху появляется выбор способа передвижения. От этого выбора будет зависеть, как будет построен маршрут. Понятное дело, что маршрут на автомобиле и пешком займет разное количество времени и проложен может быть не одинаково, машина не проедет, к примеру по лесным тропинкам. Из способов представлены автомобиль, пешеход, метро и велосипед. Маршрут для велосипеда, в отличии от автомобиля и пешехода прокладывается в обход крупных трасс, как я понял. Хотя где-то, возможно, учитываются и специализированные дорожки (там где они есть). Понятное дело, что «Метро» прокладывает путь по линиям метро, а путь от пункта отправления до вестибюля и, соответственно, от вестибюля до пункта

назначения, как для пешехода. Строка внизу предлагает добавить стартовую точку.

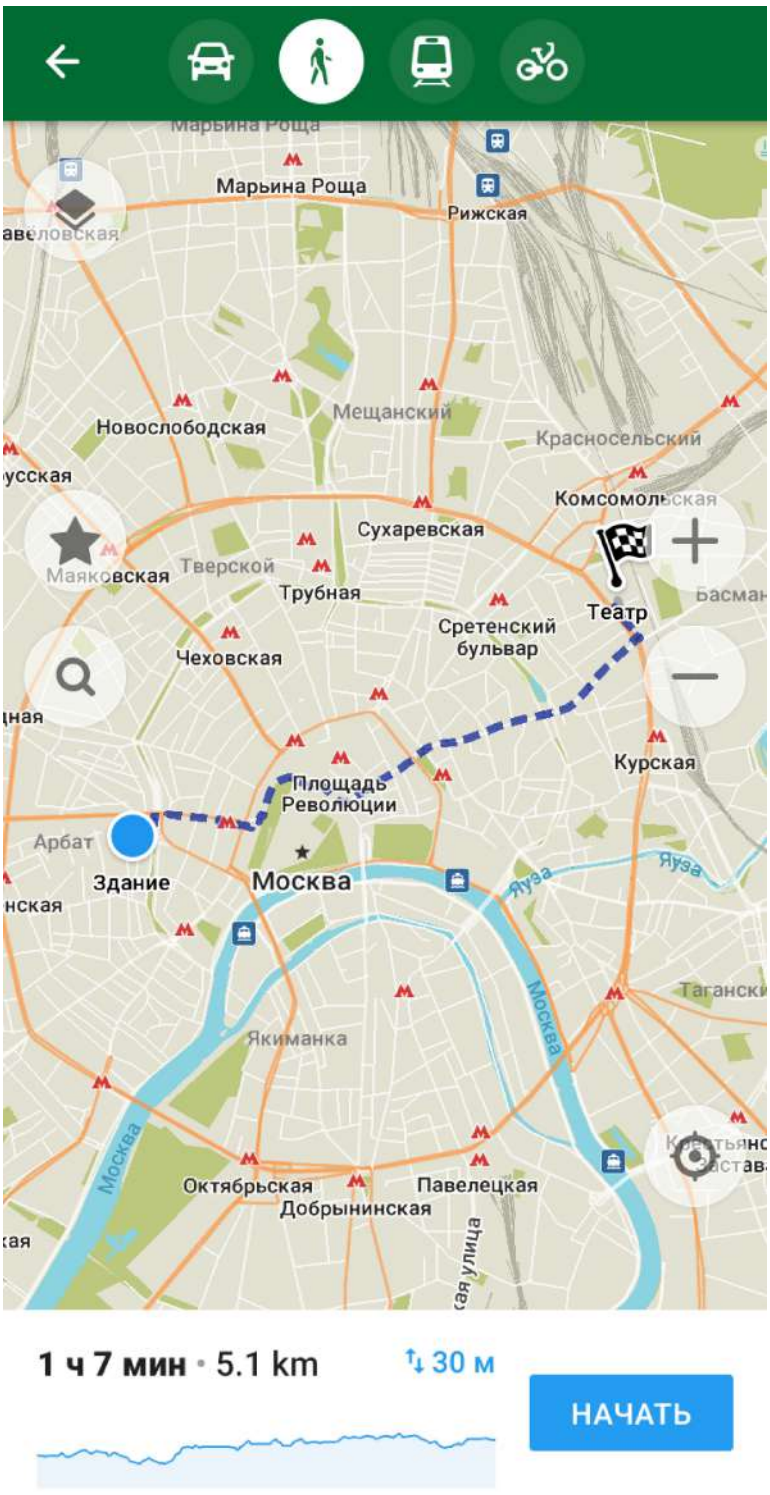
Нажимаем на нее, открывается окно поиска, и ищем с помощью него нужный адрес. Есть и другие способы его задания, например, отметить на карте нужное место и нажать «Отсюда», но с этим, я думаю, разберетесь сами. После

добавления стартовой точки, снова появляется карта и строка внизу предлагает задать конечную точку.

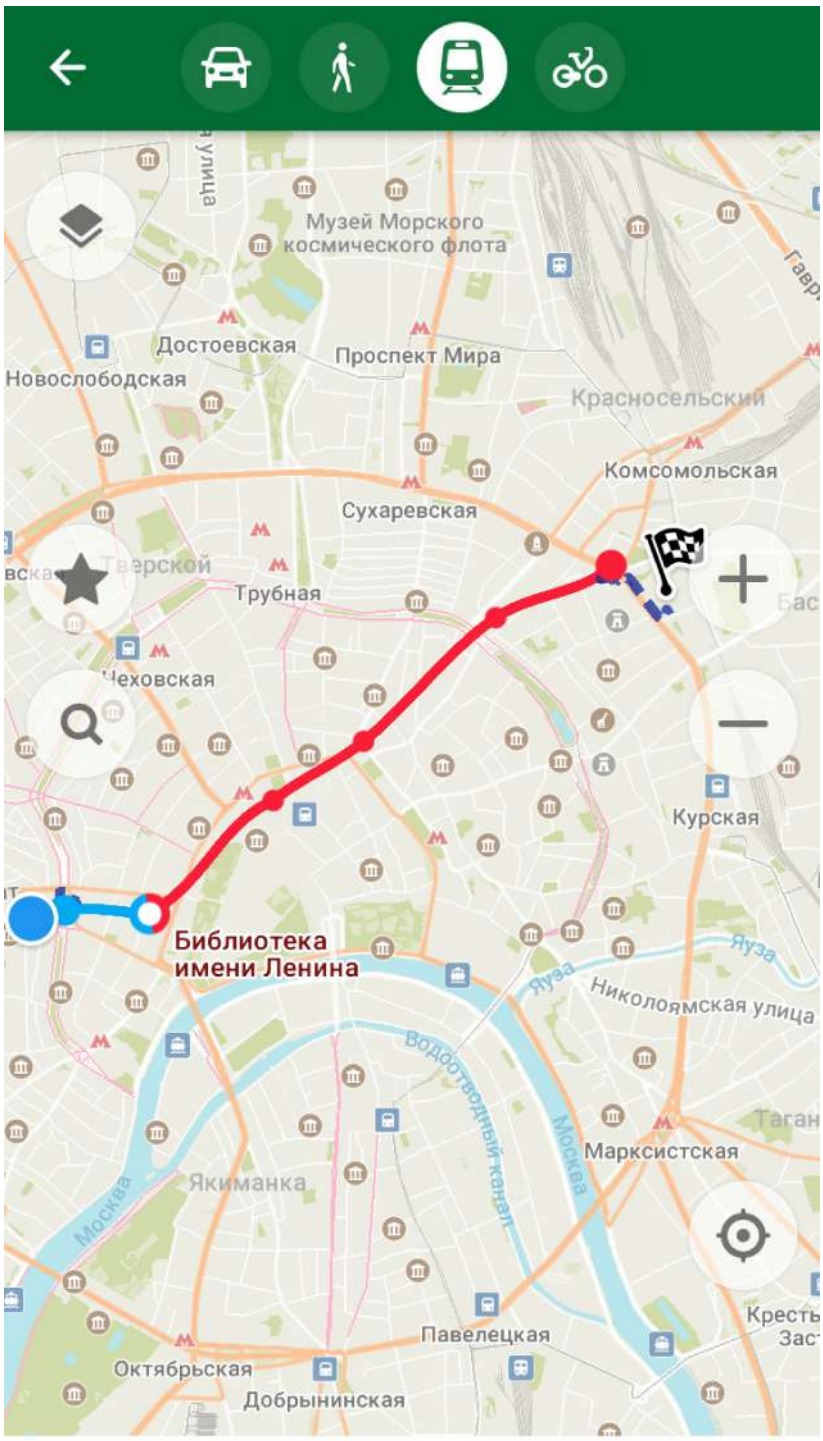
Нажимаем на нее и выбираем конечную точку аналогичным образом. После этого ждем, когда маршрут будет построен, на карте отобразится путь, а внизу появится строка, где будет указано, сколько примерно времени займет путь и какой он по протяженности в километрах.


Орнитарий
Рижская
Еврейский музей и центр толерантности
Достоевская
Проспект Мира
Новослободская
Красносельский
Комсомольская
Сухаревская
Тверской
Трубная
Театр
Сретенский бульвар
Чеховская
Курская
Площадь Революции
Музей книги
Здание
Москва
Водоотводный канал
Таганский
Якиманка
Павелецкая
Октябрьская
Добрынинская
Русские валенки
6 мин • 5.6 km
НАЧАТЬ

Разумеется, путь для автомобиля прокладывается без учета пробок. Данное приложение не поддерживает сервисы, отслеживающие состояние движения на дорогах. К сожалению, все такие сервисы несвободные. Для пешехода расчет времени производится, отталкиваясь от примерной скорости движения с учетом особенностей местности.


Марьина Роща
Рижская
Мещанский
Новослободская
Красносельский
Сухаревская
Маяковская
Тверской
Трубная
Театр
Сретенский бульвар
Чеховская
Курская
Площадь Революции
Арбат
Здание
Москва
Яуза
Таганский
Якиманка
Октябрьская
Добрынинская
Павелецкая
1 ч 7 мин • 5.1 km
30 м
НАЧАТЬ

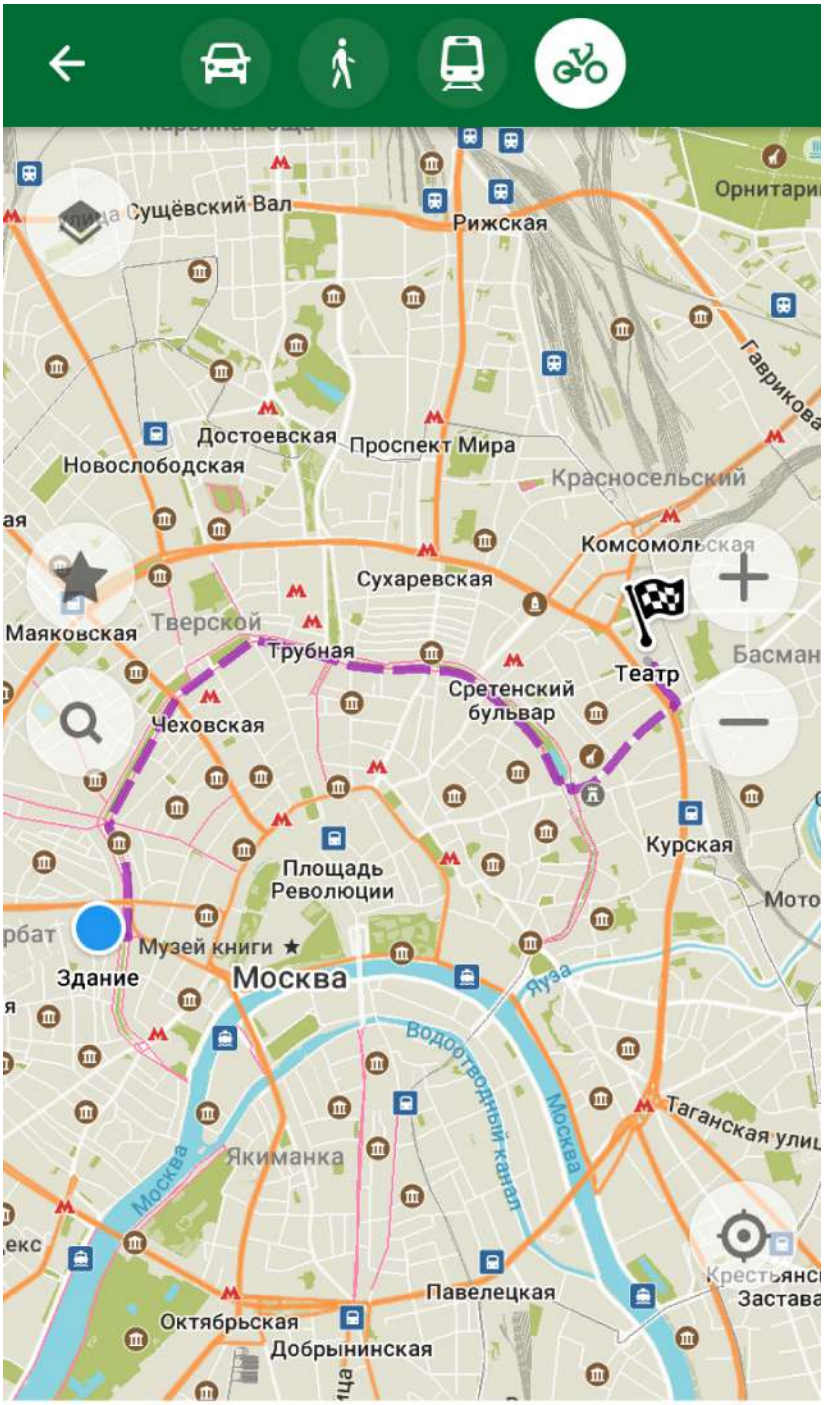
Для метро будет указано, какие ветки метро задействуются, придется ли до или от вестибюля идти пешком, а также общее расстояние в километрах, которое придется пройти.



26 мин • 1.1 km

4 • 1

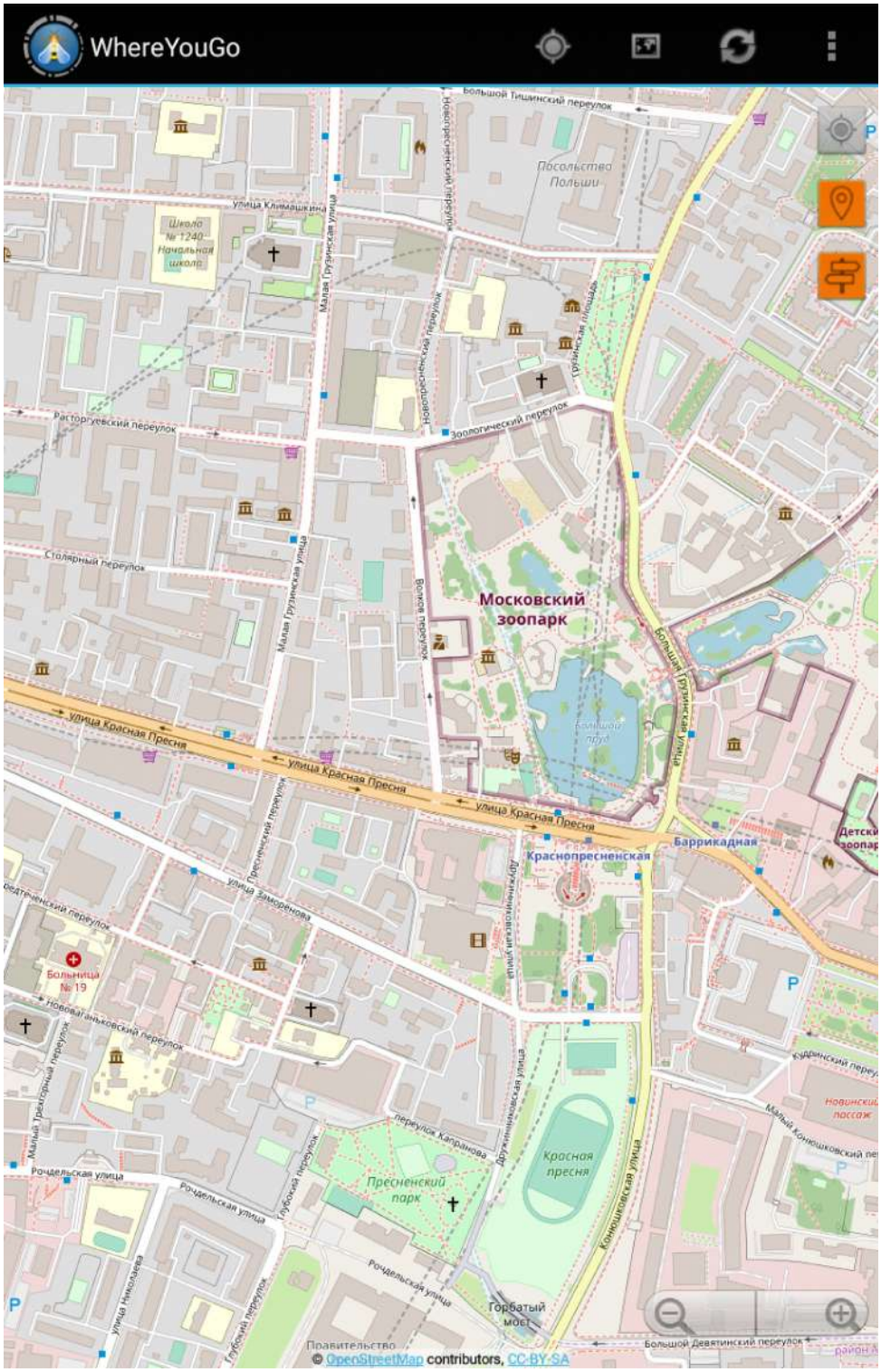
Для автомобиля, пешехода и велосипеда возможна запись пути. Для этого нужно нажать кнопку «Начать» справа на строке внизу. Напоминаю, что работать это будет только при включенной геолокации.


Сущёвский Вал
Рижская
Достоевская
Проспект Мира
Новослободская
Красносельский
Комсомольская
Сухаревская
Маяковская
Тверской
Трубная
Театр
Сретенский бульвар
Чеховская
Курская
Площадь Революции
Музей книги
Здание
Москва
Якиманка
Павелецкая
Октябрьская
Добрынинская
Таганская улиц
Басман
29 мин • 6.4 km
31 м
НАЧАТЬ

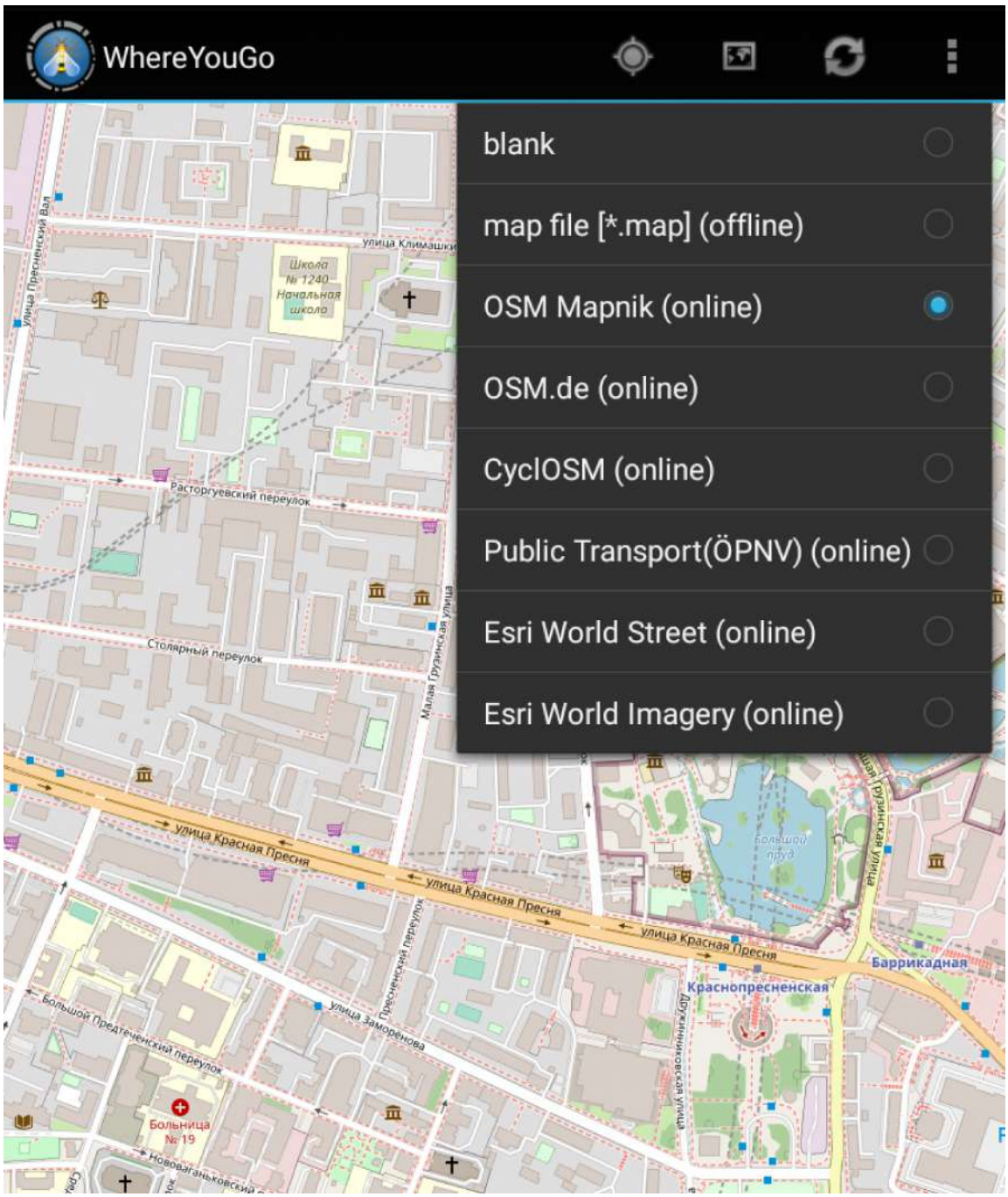
В целом, в данном приложении несложно разобраться и без инструкций. Для большинства задач, связанных с картами, его вполне хватает.

Следующим могу порекомендовать приложение WhereYouGo.[1] Оно примечательно тем, что может отображать разные виды карт. Помимо стандартных карт OpenStreetMap, также отображает множество других карт. Эти карты программа отображает онлайн, беря данные из Интернета. Однако присутствует возможность отображения и оффлайн-карт. К сожалению, само приложение не располагает функциями скачивания таких карт. Их придется скачивать отдельно, и они должны будут иметь определенный формат. Также программу можно использовать для навигации. Устанавливаем приложение и даем ему разрешение в Firewall на доступ к Интернету.

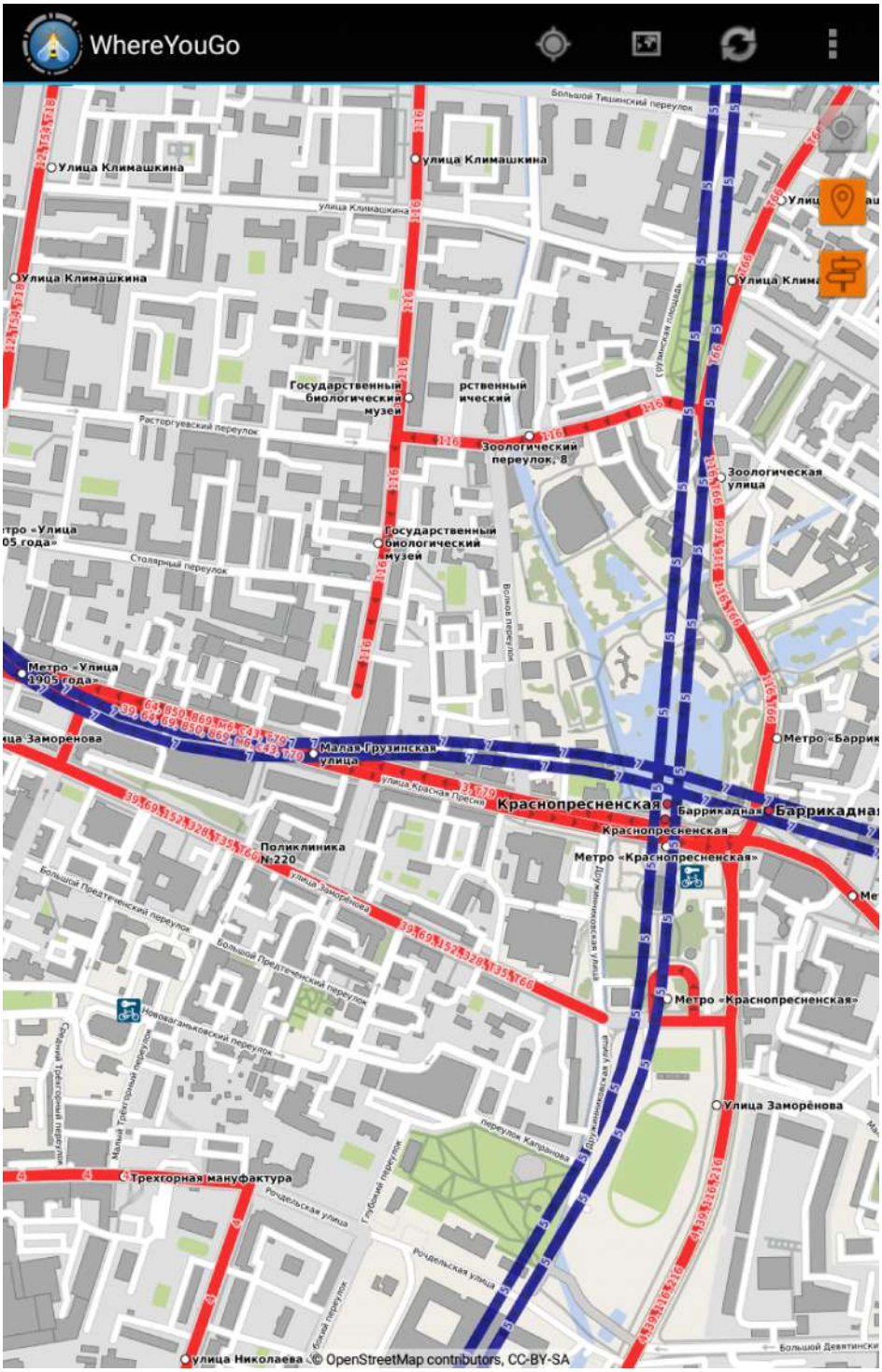
При открытии приложения, появляется окно с четырьмя иконками.
Иконка «Начало» открывает какое-то сообщение.
Иконка «Карты» открывает, собственно, карты.



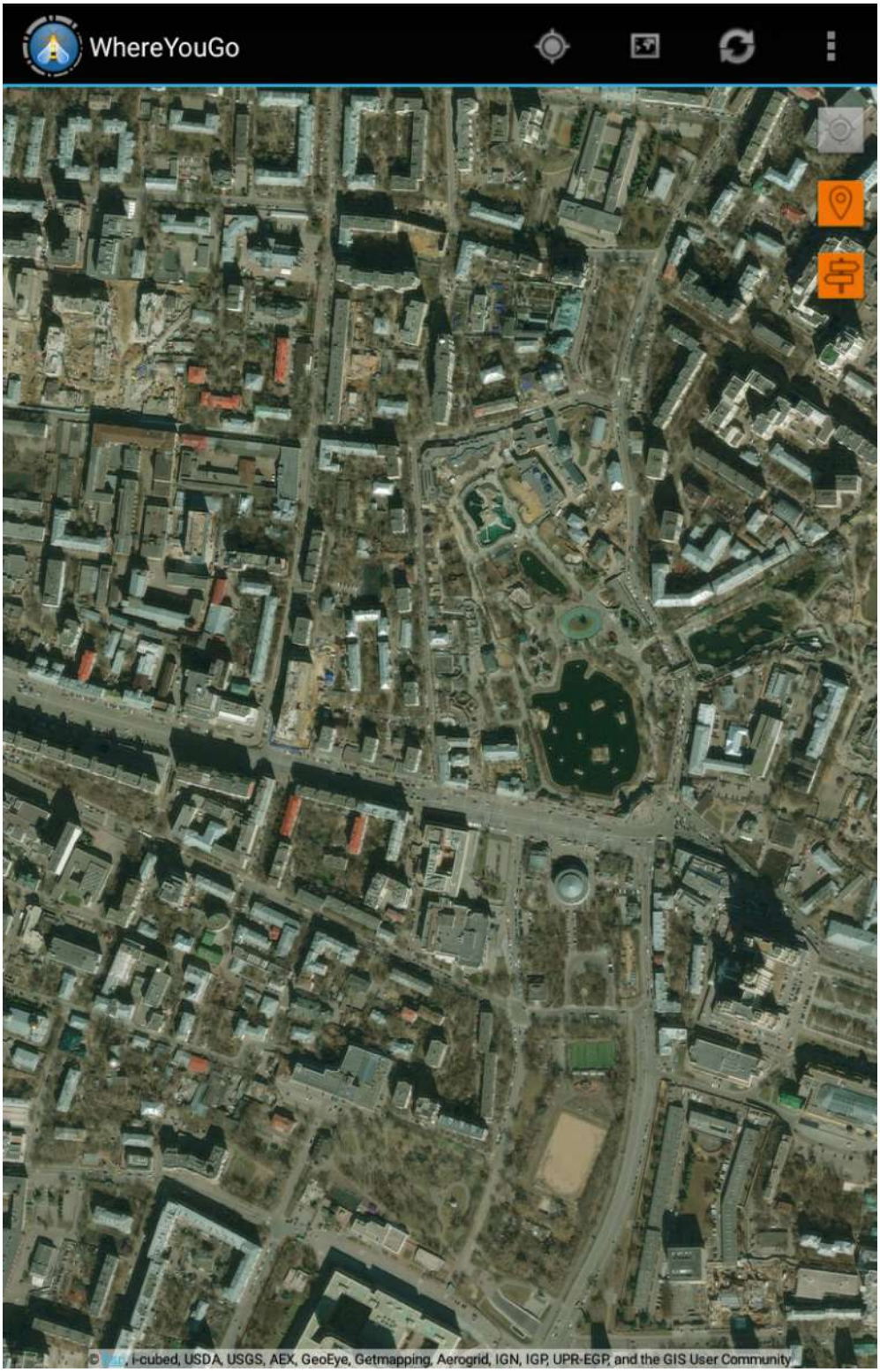
На верхней панели третий значок справа открывает список карт.



OSM Mapnik (online), это обычные карты OpenStreetMap, отображаемые из Интернета. Также, как я уже говорил, у приложения есть доступ ко многим другим видам карт, например к картам транспорта Public Transport.



И даже спутниковым снимкам Esri World Imagery.



Имейте ввиду, что не все карты могут работать.

В главном окне иконка «GPS» открывает функцию определения вашего местоположения. Понятное дело, что для этого необходимо включить геоданные.

Иконка «Настройки» открывает параметры программы, такие как настройка оповещения определения местоположения с помощью GPS, использование компаса, настройки функций навигатора, языковые настройки и т.д. На них я подробно останавливаться не буду.

Таковы возможности данной программы.

Необходимо упомянуть программу OsmAnd.[2] Эта программа достаточно известна. Она имеет наиболее широкий функционал среди открытых приложений для навигации. Позволяет использовать оффлайн-карты, самых разных типов, имеет множество функций. Однако рекомендовать ее я не могу. F-Droid указывает на множество его неприятностей. Наличие несвободных компонентов, использование несвободных сервисов, поддержка несвободных дополнений, поощрение проприетарщины, все это имеется в OsmAnd. Данное приложение может пригодится только тем, кому жизненно необходимы оффлайн не только сами карты, которые здесь, как простые, так и с общественным транспортом, но и справки Википедии. А также тем, кто жить не может без сервисов отслеживания пробок на дорогах. Приложение поддерживает сервис Яндекс.Пробки. Этот сервис, как и прочие сервисы Яндекса несвободный, и я категорически не рекомендую им пользоваться. Тем не менее, знайте, что такое приложение есть. Но все же по возможности используйте, что-то более приличное.

В качестве альтернативы можно посоветовать приложение Трекарта.[3] Но в ней, к сожалению, отсутствует прокладка маршрутов, имеется только возможность записи пути, для чего необходимо включить GPS.

Вот в принципе и все, что я хотел порекомендовать по приложениям для навигации.

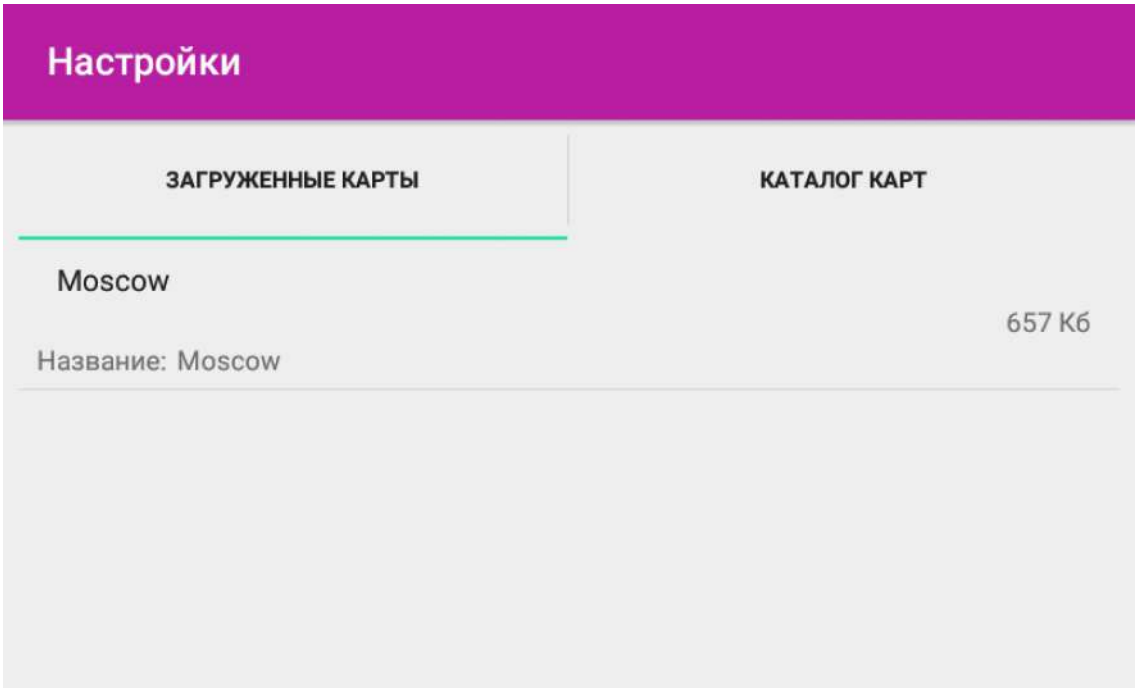
25 Карты и расписание транспорта

К сожалению, с картами и расписанием общественного транспорта в F-Droid все грустно. Приложений, которые бы качественно отображали маршруты всего транспорта, отслеживали бы прибытие и отбытие автобусов, троллейбусов и т.д., нет. Но кое-что все же можно порекомендовать.

Существует приложение pMetro.[4] Оно позволяет просматривать карты транспорта и прокладывать маршруты.

После запуска приложения откроется окно с двумя вкладками. Переходите в «Каталог карт» и нажимаете на закругленную стрелочку вверху справа.

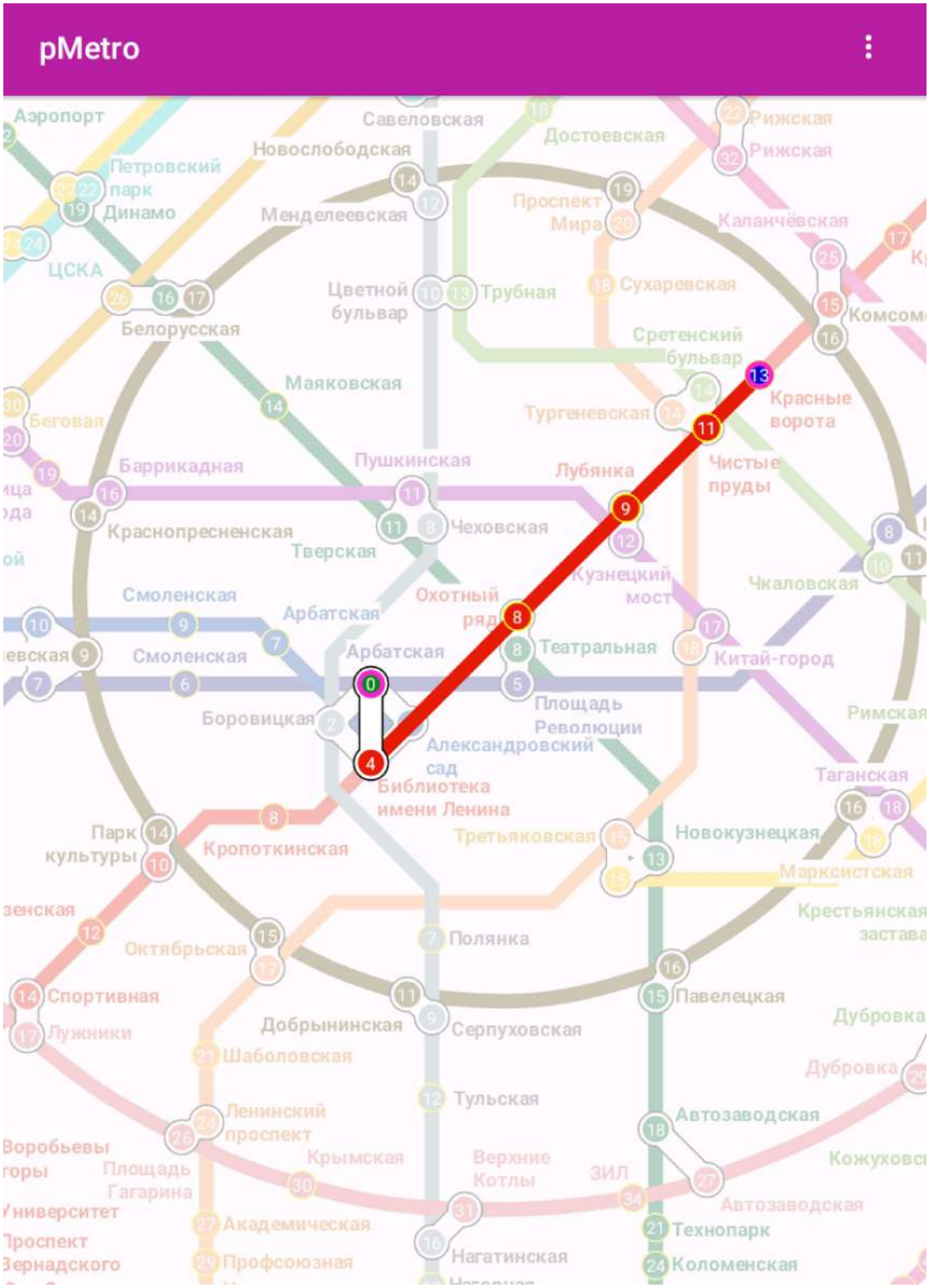
Обновится список карт. После этого выбираете свою страну, город и карту. Она загружается и появится во вкладке «Загруженные карты».



Переходите туда. Если нажать на три точки вверху справа, выскочит поле, где можно перейти на другую карту, нажав «Открыть карту», отметить транспорт для отображения, нажав «Транспорт» и перейти в параметры приложения, нажав «Настройки».

В разделе «Общие» находятся параметры отображения карт. В разделе «Карты» можно выбрать сервер, с которого будут загружаться карты, место их хранения и регулярность обновления.

Также в приложении можно прокладывать маршруты. Для этого необходимо нажать на пункт отправления (например, определенная станция), а затем на пункт назначения (также, станция). Отобразится маршрут.



На этом функционал приложения, в принципе, исчерпан.

Еще одна программа, которую можно порекомендовать, называется Transportr.[5] Она позволяет смотреть маршруты и расписания различного транспорта в разных странах. К сожалению, России в ней нет. Однако, если вы

живете в другой стране, можете поискать ее в этой программе. Также она может пригодиться вам если вы путешествуйте.

К сожалению, это все что можно порекомендовать по данной теме. Других программ с более широким функционалом мне не известно.

26 Приложения для использования Интернет-сервисов

Существуют различные приложения для использования тех или иных Интернет-сервисов. Они облегчают работу с ними.

Для измерения скорости Интернета есть приложение LibreSpeed.[6]

Для просмотра прогноза погоды наиболее предпочтительным является приложение Forecastie.[7] Отображает как текущую погоду, так и погоду на неделю с интервалом в три часа. Присутствуют подсказки и определение местоположения. Единственный минус, это отсутствие возможности создания списка городов для быстрого доступа. Если данная функция вам необходима, можете попробовать другие приложения. В качестве альтернатив можно обратить внимание на приложения Simple Weather,[8] Good Weather[9] и Weather.[10] Все они в качестве источника информации используют сервис OpenWeatherMap.[11] Это открытый сервис, который собирает и предоставляет данные по прогнозам погоды.

Для перевода с одного языка на другой есть приложение LibreTranslater,[12] которое использует сервис LibreTranslate.[13]

Для общения через обычные централизованные сервисы VoIP существует клиент Linphone.[14] В качестве альтернативы можно порекомендовать приложение Lumicall.[15]

Если хотите общаться, используя технологию Mumble, существуют клиенты Mumla[16] и Plumble.[17]

Также осуществлять аудио и видеосвязь можно с помощью инструмента Jitsi Meet.[18] . При разговоре через него лучше надевать наушники, чтобы не допустить возникновения акустической обратной связи. В остальном это прекрасный сервис, не требующий регистрации. Для создания конференции или присоединения к ней, необходимо при открытии приложения вписать название конференции в поле ввода.

Для доступа к этичным социальным сетям существуют приложения AndStatus[19] и Twitlatte.[20] Они заточены на работу с несколькими аккаунтами

в различных соц. сетях. Также их можно использовать для доступа к неэтичному сервису Twitter. Разумеется для доступа к отдельным соц. сетям существует множество специальных приложений.

Если вам необходимо по каким-то причинам использовать неэтичную социальную сеть Facebook, то можно это делать через свободные приложения, такие как Frost for Facebook,[21] SlimSocial for Facebook,[22] MaterialFBook,[23] Face Slim,[24] Tinfoil for Facebook[25] и Toffeed.[1]

Если необходим доступ к Twitter, то также существуют свободные клиенты SlimSocial for Twitter[2] и Tinfoil for Twitter.[3]

Если нужен доступ к Instagram, то есть приложение Barinsta.[4] Также для скачивания и репоста материалов Instagram, можно воспользоваться программой Easy Repost.[5]

Для доступа к видеохостингу YouTube можно воспользоваться приложением NewPipe.[6] В этой программе, помимо просмотра, хорошо реализована функция скачивания видео. В качестве альтернативы можно указать приложение WebTube.[7] Еще есть программа YouTube Stream,[8] для просмотра стримов на YouTube. Помимо этого существует приложение YaShlang.[9]

Разумеется, это далеко не полный список приложений в F-Droid для доступа к различным Интернет-сервисом. Но этого достаточно для простого пользователя.

27 Приложение MEGA

Для управления папками и файлами в удаленном хранилище MEGA, а также для общения, можно воспользоваться приложением с одноименным названием.[10] К сожалению, из-за того, что соглашения MEGA налагают определенные ограничения на коммерческое распространение копий исходного кода, приложение не может попасть в F-Droid. И скачать его отдельно с сайта нельзя. Скачать его можно лишь с репозиториев Google. Безусловно, обращаться к Play-маркету недопустимо. К счастью, существует свободное приложение, позволяющее скачивать ПО с хранилищ корпорации без его использования. Оно называется Aurora Store и присутствует в F-Droid.[11] Устанавливаем его.

Открываем приложение и первым делом необходимо выбрать способ установки. Я рекомендую оставить его по-умолчанию. В некоторых версиях мобильных систем, установка таким способом может нарваться на некоторые препятствия. Однако обычно приложение четко о них сообщает и дает конкретные указания, как это исправить.

Далее выбираем тему. Затем будет предложена работа через аккаунт Google или анонимный режим. Нажимаем «Анонимно».

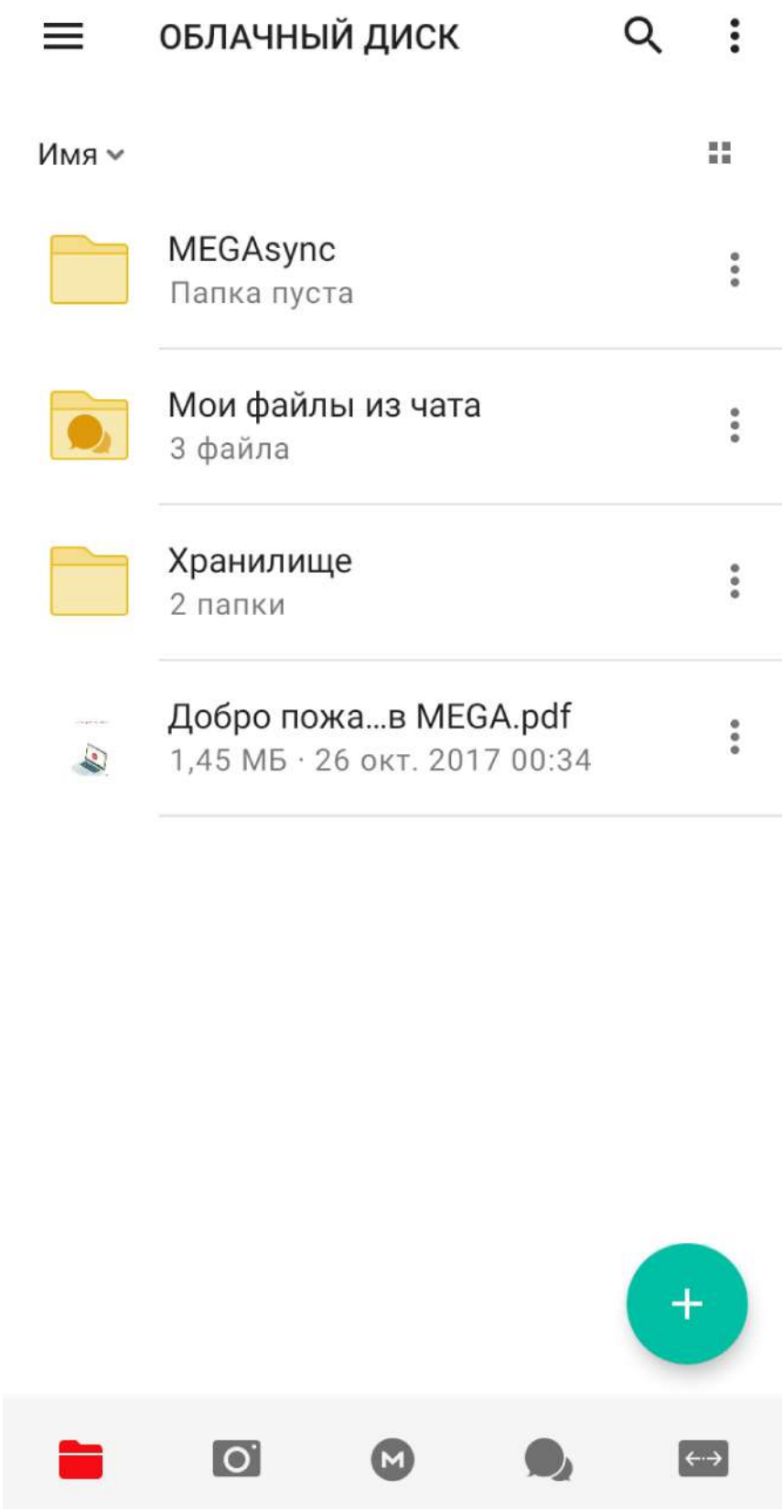
Открывается основное окно приложения. Нажимаем на значок с лупой внизу справа и в появившемся наверху поле вводим «MEGA». Нужное приложение будет на самом верху, под названием у него будет надпись «Mega Ltd». Нажимаем на него и затем нажимаем на синюю кнопку «Установить» внизу. Начнется скачивание и установка. Это может занять время. Ждем до тех пор, пока надпись на синей кнопке внизу не сменится на «Открыть».

После этого закрываем Aurora Store и открываем MEGA, дав ей предварительно разрешение на доступ к Интернету. В появившемся окне

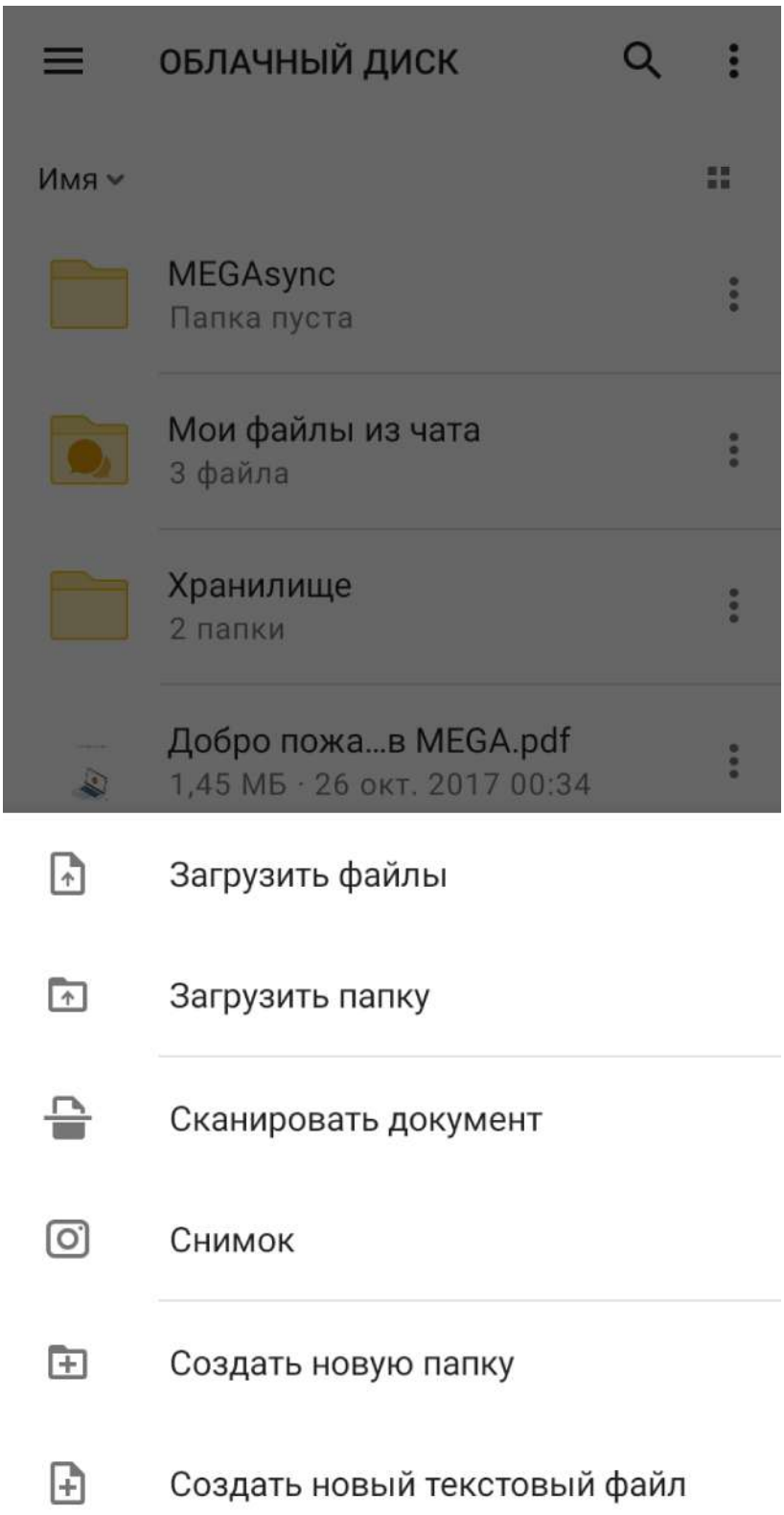
предлагается ввести логин и пароль. Указываем их, а если аккаунта еще нет, то нажимаете на кнопку «Зарегистрироваться» и проходите процесс регистрации. Откроется окно, в котором будет спрашиваться о том, какой раздел открывать при запуске приложения. Тут выбираете по своим нуждам. Если собираетесь активно использовать его для общения, то можете указать чат. Откроется основное окно программы, тот раздел, который вы выбрали.

Основное окно состоит из пяти вкладок, переключение между которыми осуществляется на панели внизу.

Слева значок папки — это ваше удаленное хранилище. Здесь вы можете работать со своими папками и файлами.



Если нажать на три точки справа от папки или файла снизу вылезет список возможных действий, включая управление ссылкой и открытие общего доступа (для папок). Чтобы загрузить новый файл, нажимаем на зеленый значок «плюс» внизу справа и выбираем «Загрузить файлы».

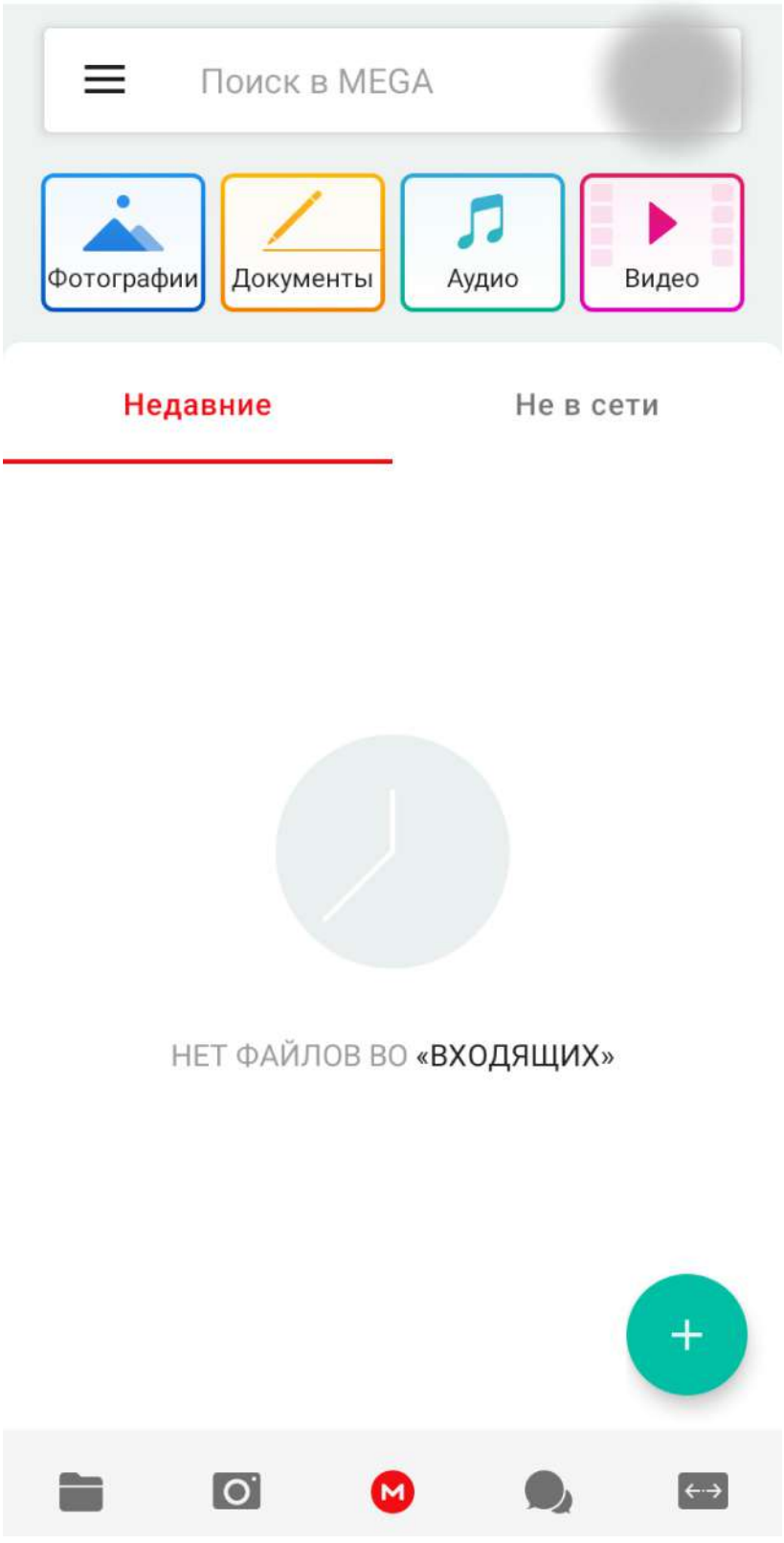

ОБЛАЧНЫЙ ДИСК
Имя
MEGAsync
Папка пуста
Мои файлы из чата
3 файла
Хранилище
2 папки
Добро пожа...в MEGA.pdf
1,45 МБ · 26 окт. 2017 00:34
Загрузить файлы
Загрузить папку
Сканировать документ
Снимок
Создать новую папку
Создать новый текстовый файл

Открывается окно файлового менеджера, где необходимо выбрать файлы для загрузки и нажать «Открыть». Файлы будут помещены в удаленное хранилище.

Таким же способом можно создавать новые папки.

Вторая вкладка слева внизу со значком камеры, это загрузка фотографий непосредственно с камеры. Если эту функцию активировать, то вы сможете отснятые материалы помещать сразу же в удаленное хранилище. Если вам нужен такой функционал, можете пользоваться.

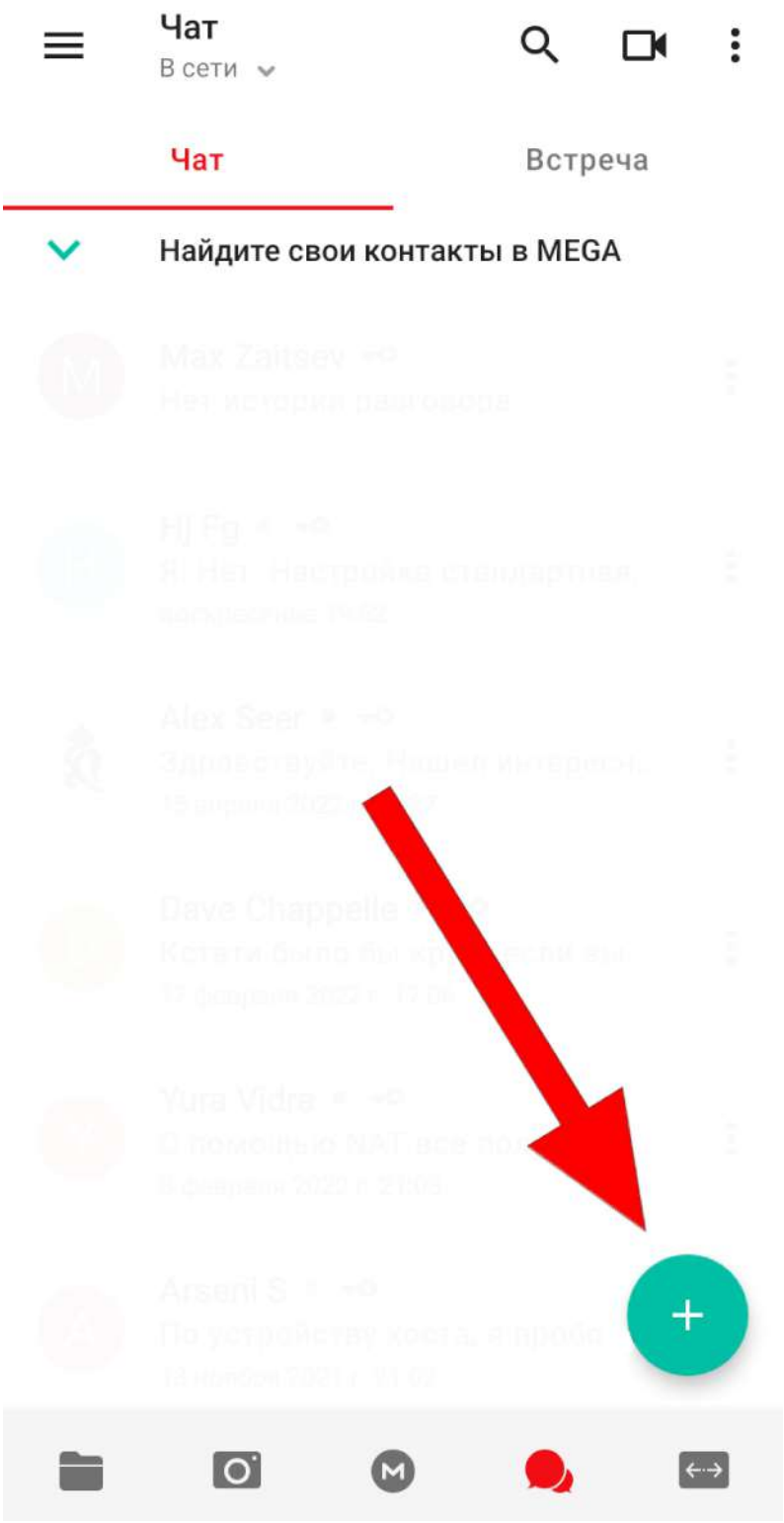
Третья вкладка внизу — по центру — это недавние файлы помещенные в хранилище. Здесь вверху также есть быстрый доступ к различным типам файлов, лежащих в хранилище.



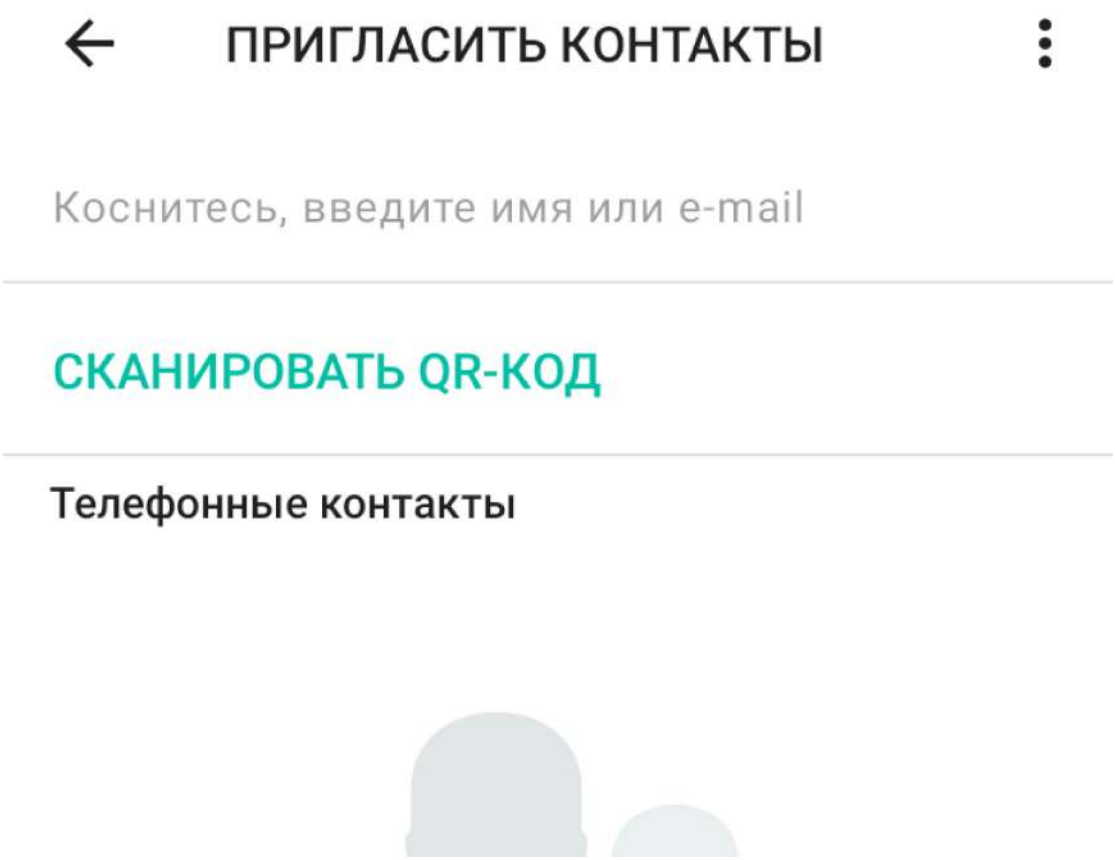
Четвертая вкладка, это мессенджер. Здесь можно добавлять собеседников, создавать группы и присоединяться к существующим. Можно обмениваться сообщениями, файлами, совершать голосовые и видеозвонки, проводить конференции. К этой вкладке мы еще вернемся.

В последней вкладке отображаются общие папки. Здесь также есть три вкладки. «Входящие», это папки, созданные другими, к которым есть доступ у вас. «Исходящие», это папки, которые создали вы, и открыли для общего доступа. «Ссылки», это быстрый доступ к файлам, для которых вы создали ссылки, которыми можно делиться с другими.

Сейчас я подробнее разберу вопрос общения через данное приложение. Идем в соответствующую вкладку. Здесь есть два раздела — «Чат» и «Встреча». В первом отображаются индивидуальные и групповые чаты, во втором конференции. Чтобы добавить собеседника, будучи в разделе «Чат», нажимаем на зеленый значок «плюс» внизу справа.



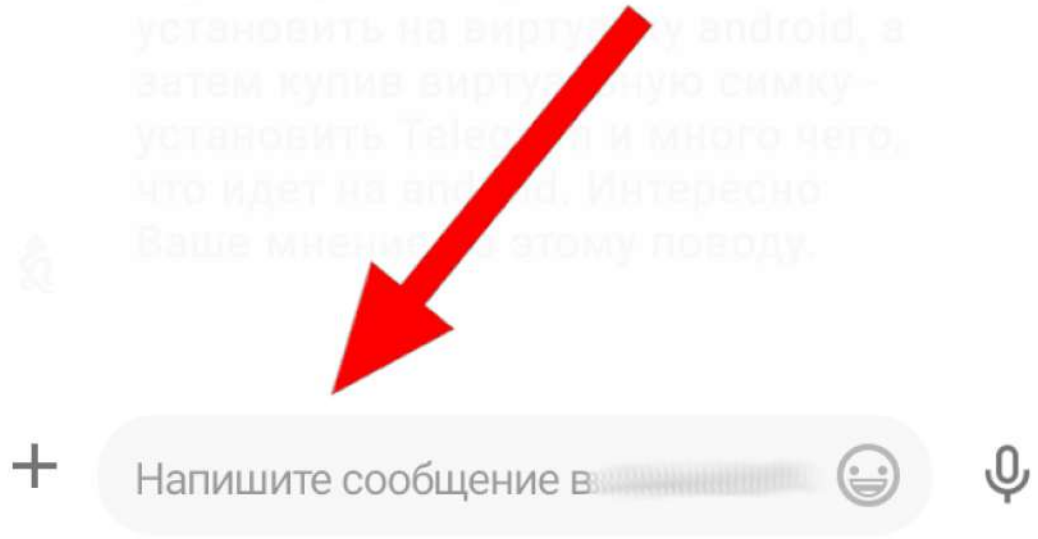
Нажимаем «Новый чат». Выбираем «Пригласить контакты». Если у вас есть QR-код собеседника, может нажать «Сканировать QR-код» и, наведя на него камеру, добавить контакт. В ином случае в верхнем поле необходимо ввести адрес электронной почты, являющийся идентификатором собеседника в MEGA. После чего нажать значок самолетика внизу справа.



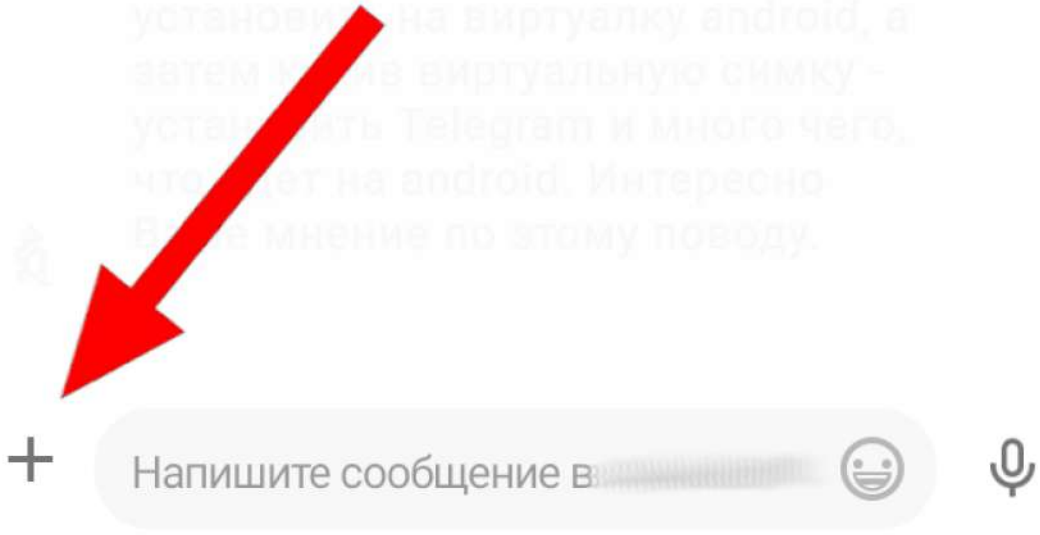
Контакту будет отправлен запрос. Если он его примет, то появится возможность вести переписку.

Если вам пришел запрос в контакты, это появится во вкладке полученных запросов в разделе «Контакты». Который можно открыть нажав на три полоски вверху справа и выбрав «Контакты», а затем «Запросы». Чтобы принять запрос, нажимаем на него и затем нажимаем «Принять». Если нажать на контакт, то откроется информация о нем. Здесь же можно подтвердить учетные данные контакта, с помощью подтверждающего ключа. Здесь отображаются данные как собеседника, так и вас. Процедуру подтверждения я уже описывал, когда говорил об общении через MEGA на компьютере, и сейчас повторяться не буду.

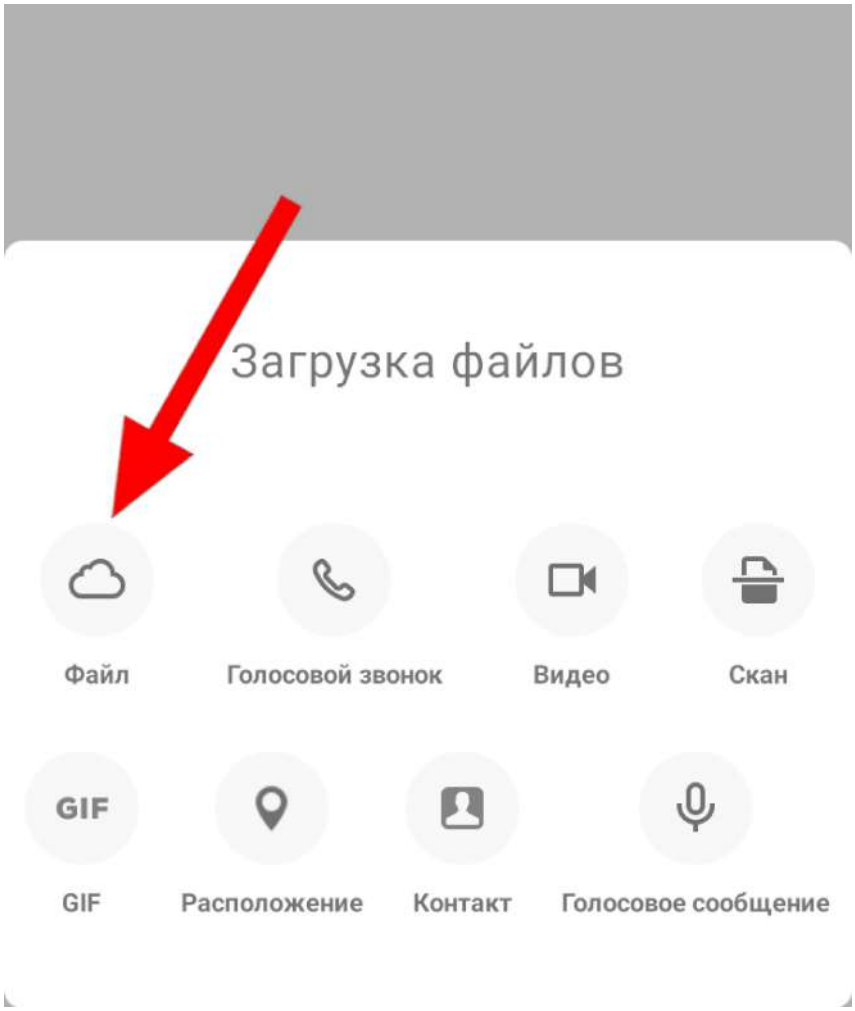
После того, как контакт добавлен, он появляется во вкладке чатов. Нажимаем на него. Чтобы отправить сообщение, наберите его в поле внизу и нажмите значок самолетика справа от него.



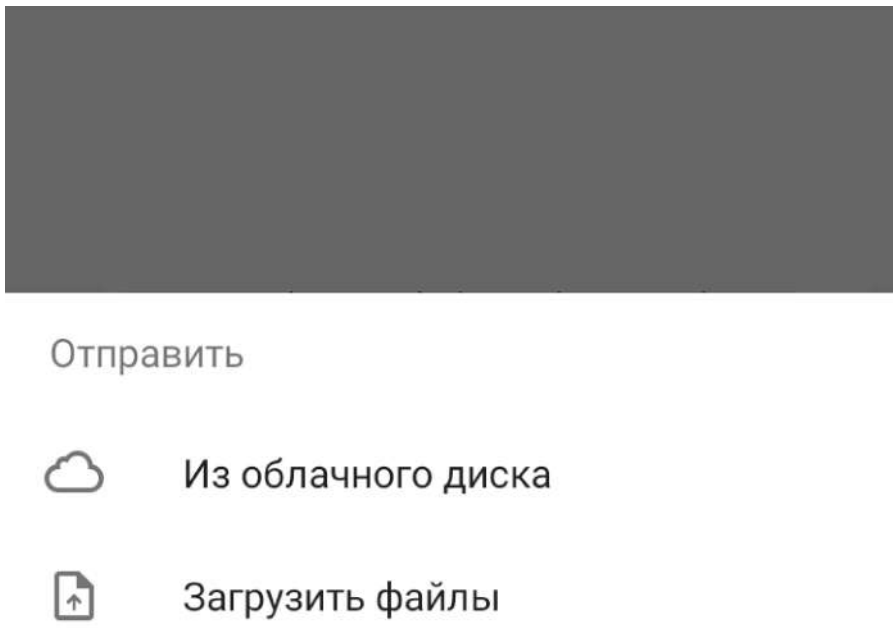
Чтобы отправить файл, нажмите на значок «плюс» внизу слева.



Выберите «Файл».



Выберите, откуда взять файл — из облачного диска или из файловой системы.

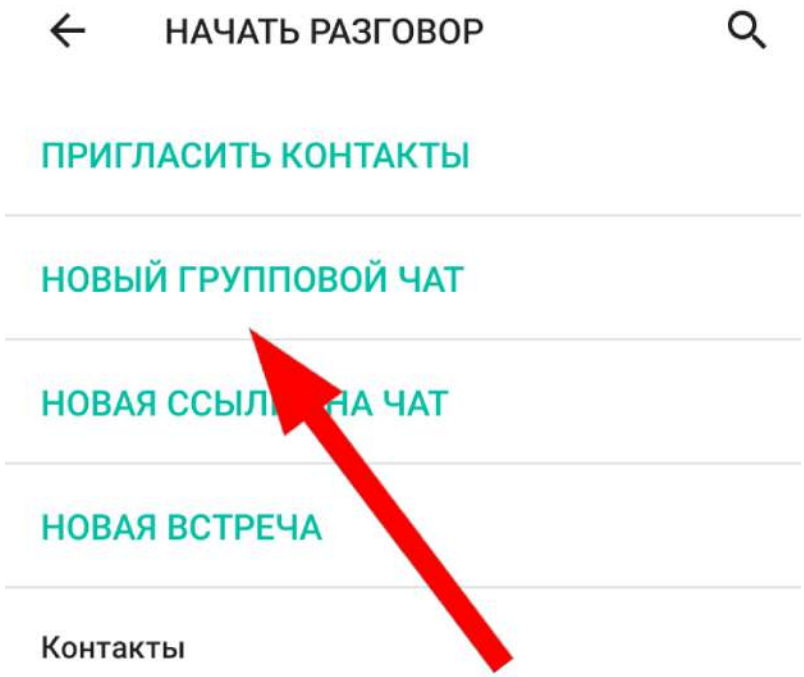


Далее из появившегося списка приложений нужно выбрать файловый менеджер. Он откроется, и необходимо будет выбрать нужный файл, после чего нажать «Открыть». Файл будет отправлен.

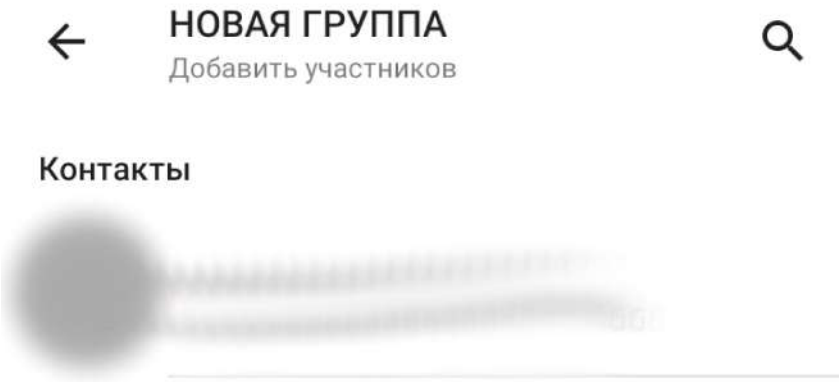
Чтобы сделать аудиозвонок, нажмите на значок телефонной трубки вверху справа.

Чтобы совершить видеозвонок, нажмите на значок камеры вверху справа.

Чтобы создать группу, нажмите в вкладке чатов на зеленый значок «плюс» внизу справа и выберите «Новый групповой чат».



Затем нужно выбрать участников чата из ваших контактов.



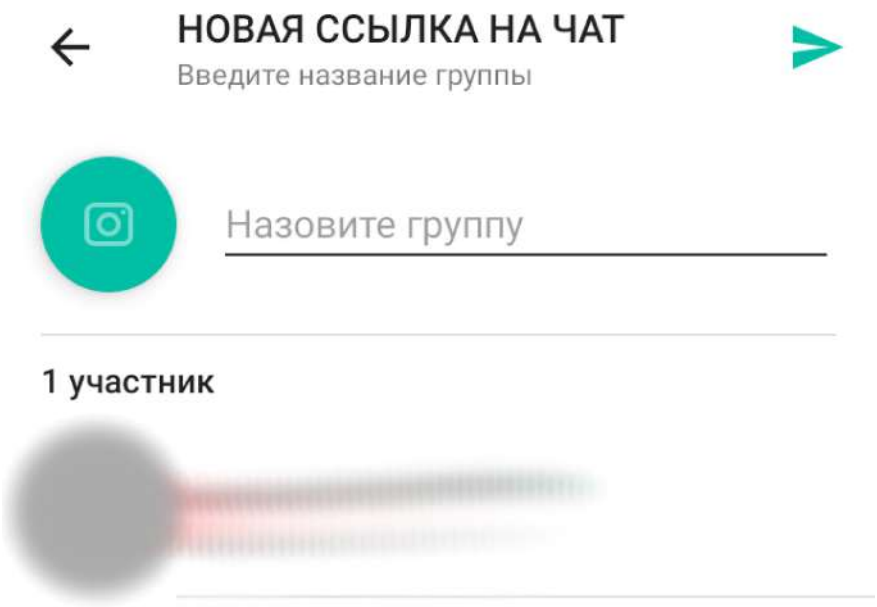
Затем добавить название группы. Чат будет создан. Чтобы отправить кому-то ссылку на этот чат, будучи в нем, нажмите на три точки справа сверху и выберите «Ссылка на чат».

Внизу всплывет список действий, выберите «Скопировать ссылку» и отправьте ее тем или иным образом тому, кого хотите пригласить. Или разместите ее, где вам нужно.

Отправка сообщений и файлов в нем осуществляются аналогично тому, как в переписках с отдельными собеседниками.

Некоторая разница присутствует в звонках — конференциях. Чтобы начать конференцию, нажмите на значок телефонной трубки вверху справа. По-умолчанию, она начинается в аудиорежиме, но вы и другие участники можете по желанию активировать свои камеры. Для отображения доступно не более шести камер.

Чтобы присоединиться к существующей группе, нажмите во вкладке чатов на зеленый значок «плюс» внизу справа и выберите «Новая ссылка на чат». Здесь в верхнем поле необходимо ввести ссылку на групповой чат, к которому вы хотите присоединиться. После этого группа появится в общем списке чатов.



Таков функционал данного приложения.

28 Двухфакторная аутентификация

Весьма серьезно повысить безопасность ваших аккаунтов способна двухфакторная аутентификация.[12] Методов аутентификации довольно много. Существует, например, биометрия и USB-ключи. Биометрия, конкретно сканирование отпечатков пальцев, сейчас не является экзотикой и присутствует во многих смартфонах. Однако, я не рекомендую ей пользоваться — незачем подвергать свои отпечатки опасности слива. USB-ключи, это уже достаточно сложный метод и рекомендовать его широкой аудитории не приходится. Для простого пользователя, таким образом, остаются доступными два метода — одноразовые коды, присылаемые через SMS, или генерируемые специальными приложениями.[13]

По поводу аутентификация с помощью SMS пояснять особо нечего. Сервис генерирует случайный код и отправляет его в SMS. Вы этот код вводите, сервис сверяет введенный вами код с тем, который он сгенерировал и послал на привязанный к вашему аккаунту телефон, если они совпадают —

аутентификация проходит успешно.

С аутентификацией через приложение все несколько сложнее. В этом случае сервис генерирует секретный ключ, который вам необходимо импортировать в приложение и на основании этого ключа, ориентируясь на время в определенной системе отсчета (есть еще вариант ориентации на факт аутентификации, но он сейчас применяется реже), приложение будут генерировать одноразовые коды. Сервис, в свою очередь, также генерирует коды, отталкиваясь от параметра времени. Таким образом, приложения, имея секретный ключ и счетчик времени, генерирует коды, и сервер, также имея секретный ключ и свой счетчик времени, также генерирует коды. Поскольку и приложением и сервисом используется отсчет времени в определенной системе отсчета, коды получаются одинаковыми.[14] Теоретически, конечно, может произойти рассинхронизация, и тогда вы не сможете войти в свой аккаунт. Но вероятность такого крайне мала.

У обоих способов — SMS и приложений — есть свои преимущества и недостатки.[15]

В случае одноразовых кодов, присылаемых через SMS, вам необходимо предоставить сервису свой номер телефона, а это уже потенциальная проблема, т.к. обладание вашим номером открывает дополнительные каналы для атак. В случае приложения, сливать номер телефона нет необходимости.

Однако в случае, когда злоумышленник пытается взломать ваш аккаунт, не зная, что используется двухфакторная аутентификация, SMS вас обязательно оповестит о попытке входа, и вы узнаете, что вас пытаются взломать. В случае же с приложением, такого нет. Ничто вас не предупредит о попытке взлома. Исключением являются случаи, когда ваш аккаунт привязан к телефону, почте или другому аккаунту, и на сервисе отдельно настраивается оповещение о любой попытке входа в систему.

Что касается перехвата одноразовых паролей. Чтобы перехватить SMS с паролем злоумышленнику нужно эксплуатировать уязвимости комплекта протоколов ОКС 7, о которых уже говорилось. Для того, чтобы это сделать, ему необходим доступ к шлюзу ОКС 7. Далеко не каждый злоумышленник сможет его получить. Еще одним вариантом является копия SIM-карты. В этом случае взломщик обращается к оператору, выдавая себя за вас, и просит перевыпустить SIM-карту, с номером, которым пользуйтесь вы. Если ему это удается, то SMS с кодом будут приходить ему.[16] Также злоумышленник может внедрить в

телефон на стадии его производства или транспортировки вирус, который будет перехватывать входящие SMS и отсылать их ему. В случае приложения, взломщику необходимо перехватить одноразовый код, который вы послали на сервер и успеть ввести его до того, как истечет срок его действия (обычно 30 секунд). Для всего этого ему также необходимо преодолеть шифрование канала, по которому осуществляется передача кода от вас до сервиса. Это задача, мягко говоря не из легких.

Что касается взлома устройства. Если вы используйте одно и тоже оборудование для аутентификации и для получения SMS, то у злоумышленника есть единая точка компрометации. Соответственно, взломав ваше устройство, он получит возможность попасть в ваш аккаунт. Если вы используйте одно оборудование для аутентификации и приложения, генерирующего коды, то у взломщика также единая точка компрометации со всеми вытекающими. Поэтому желательно приобрести отдельное устройство для SMS или приложения с кодами. Для SMS можно купить обычный кнопочный телефон, который стоит недорого. Смартфон же для приложения обойдется гораздо дороже.

Касательно взлома сервера. В случае SMS, сервер генерирует просто случайное число, поэтому взломав его, злоумышленник не получит информации, которая позволит ему предугадать следующий код, и таким образом, получить доступ к аккаунту. В случае же приложения, существует единый секретный ключ, хранящийся на сервере и в приложении. Взломав сервер, злоумышленник может получить этот ключ, что позволит ему предугадать следующий код и проникнуть в ваш аккаунт.

Несмотря на то, что от взлома через сервер аутентификация через SMS лучше защищена и от взлома через устройство обезопасится легче, я лично считаю приложения более предпочтительным вариантом. От перехвата этот способ защищен, как минимум, не хуже, а главное, не требует, в обязательном порядке, сливать свой номер телефона.

Поскольку давать инструкцию по использованию аутентификации через SMS нет нужды — она совершенно тривиальна, я покажу как пользоваться наиболее приглядными приложениями для аутентификации.

Первое приложение, которое я хотел бы порекомендовать, это Aegis.[17] Оно весьма удобное и позволяет дополнительно зашифровать себя с помощью пароля, что дает дополнительную защиту в случае взлома устройства.

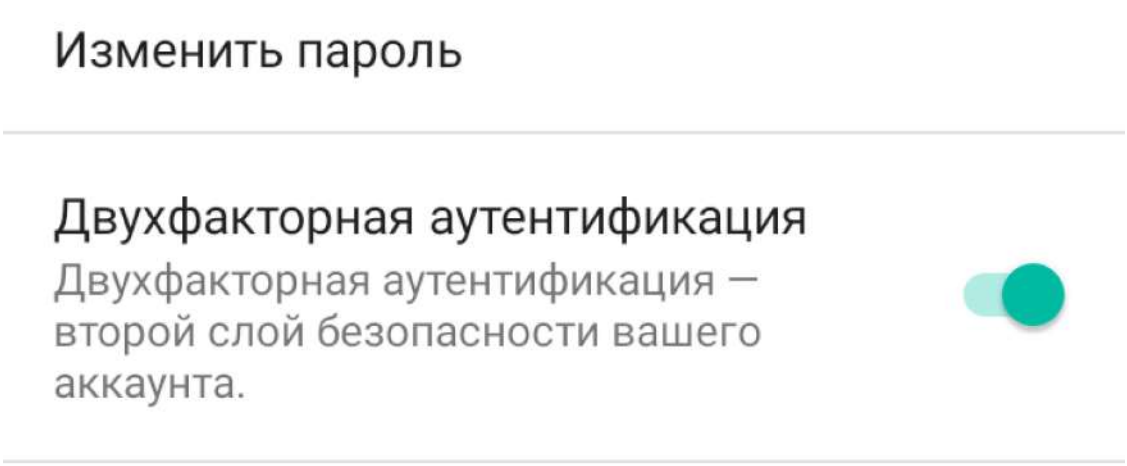
Скачиваем его из F-Droid.

При открытии приложение сразу предлагает указать пароль шифрования. Я рекомендую задать его.

Открывается основное окно приложения. Если нажав на три точки справа сверху, можно пройти в настройки. Здесь все задаете по своим потребностям.

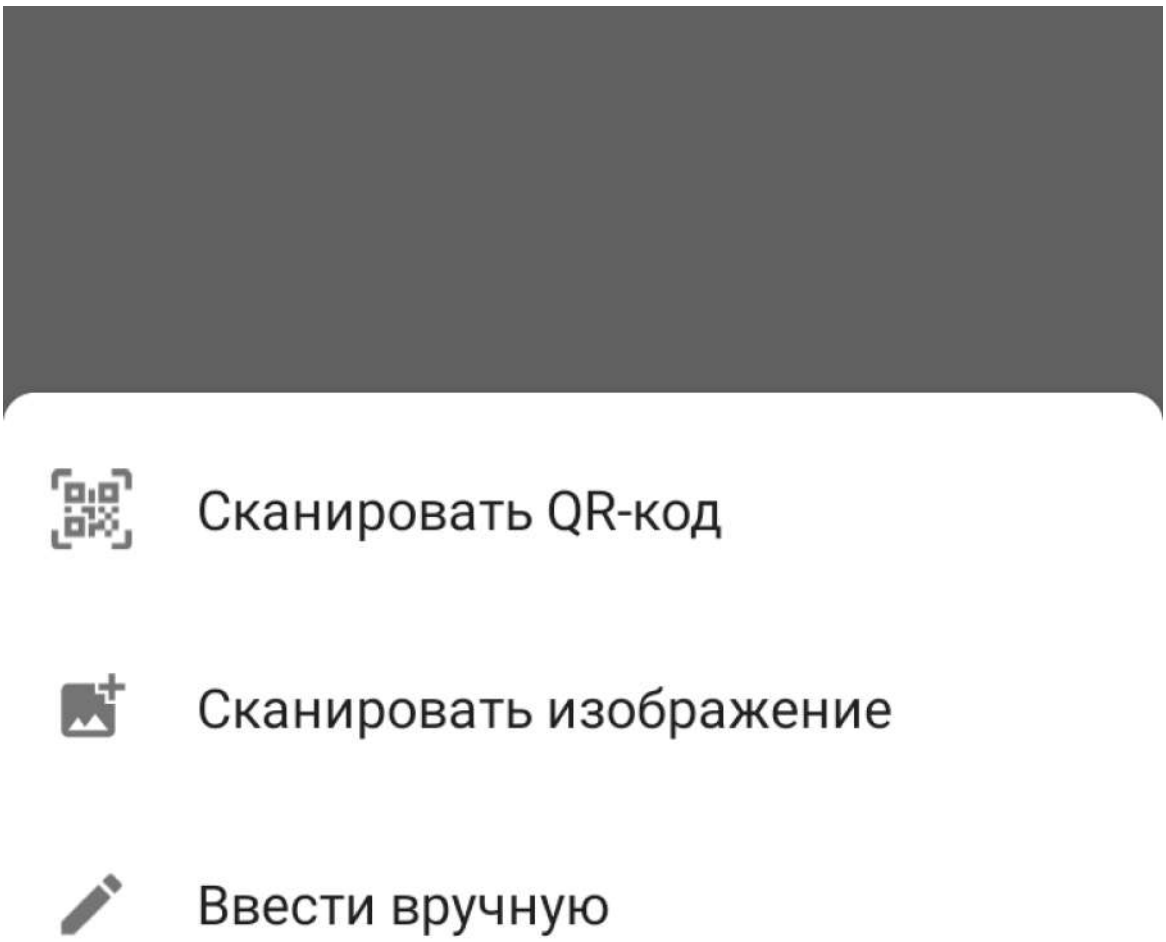
Использование двухфакторной аутентификации я покажу на примере подключения данной функции в MEGA. Открываем приложение MEGA, нажимаем на три полоски слева вверху и затем нажимаем «Настройки».

Здесь в графе «Двухфакторная аутентификация» активируем ползунок.

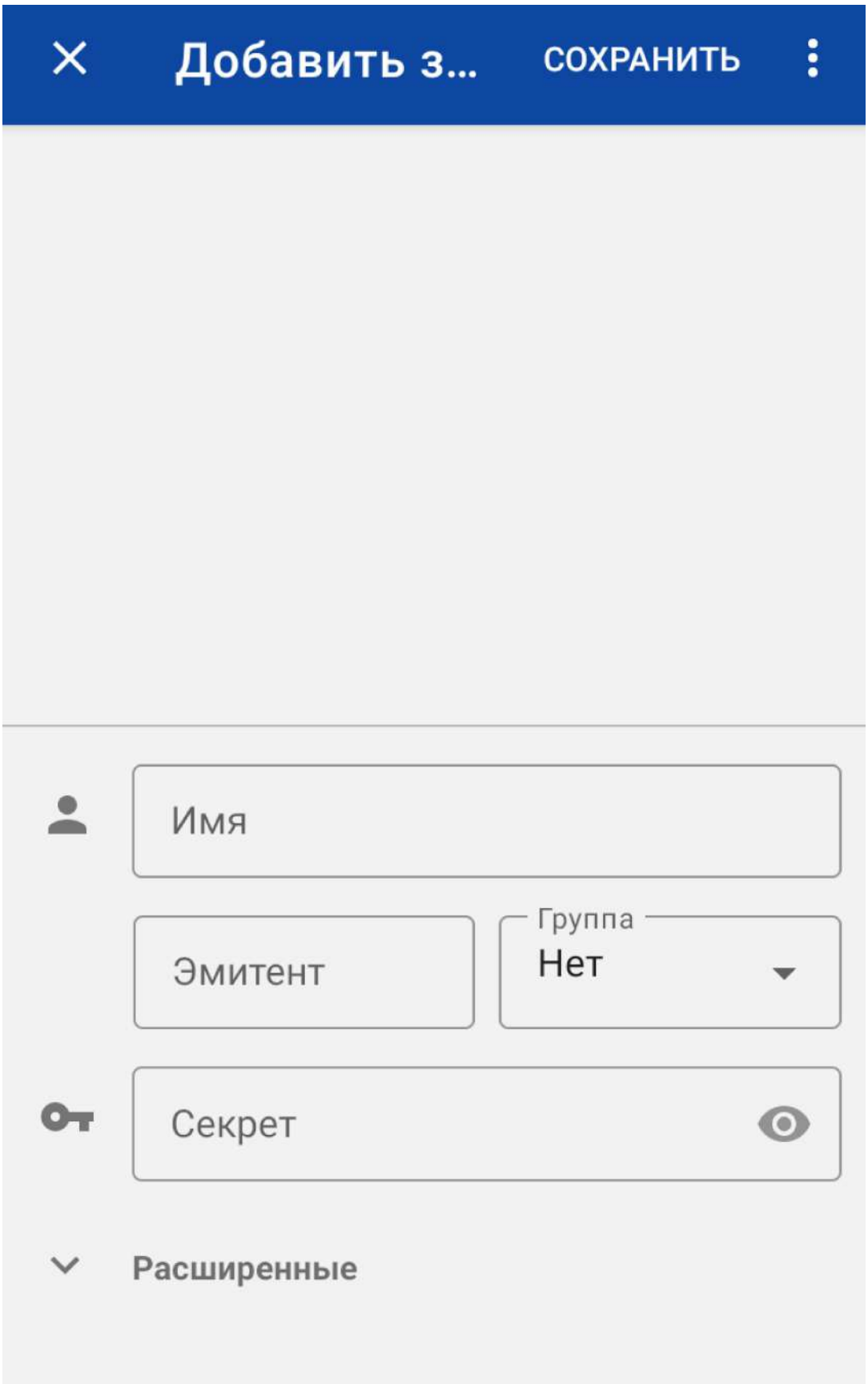


Появится окно со сгенерированным секретным ключом.

Чтобы добавить его в приложение для генерации кодов, копируем его, долгим нажатием, переходим в Aegis и здесь нажимаем на синий значек «плюс» внизу справа. После чего выбираем «Ввести вручную».

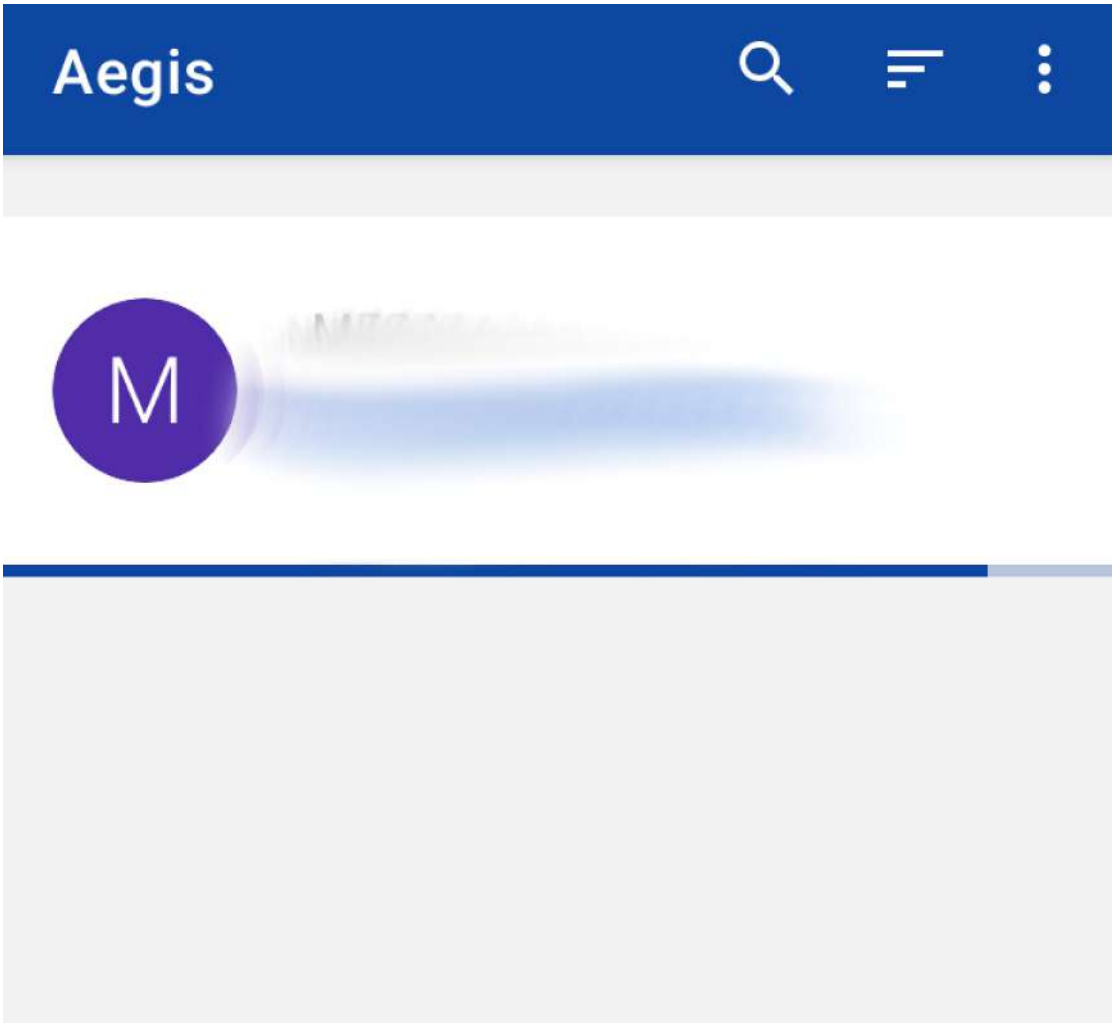


В открывшемся окне в поле «Имя» указываем название сервиса или свой ник, а в поле «Секретный ключ» вставляем скопированный ключ, для чего производим долгое нажатие на поле и нажимаем среди выскочивших надписей «Вставить».



После чего нажимаем «Сохранить» вверху справа.

В основном окне появится запись с кодом, который будет меняться каждые полминуты. Именно этот код и нужно вводить при аутентификации.

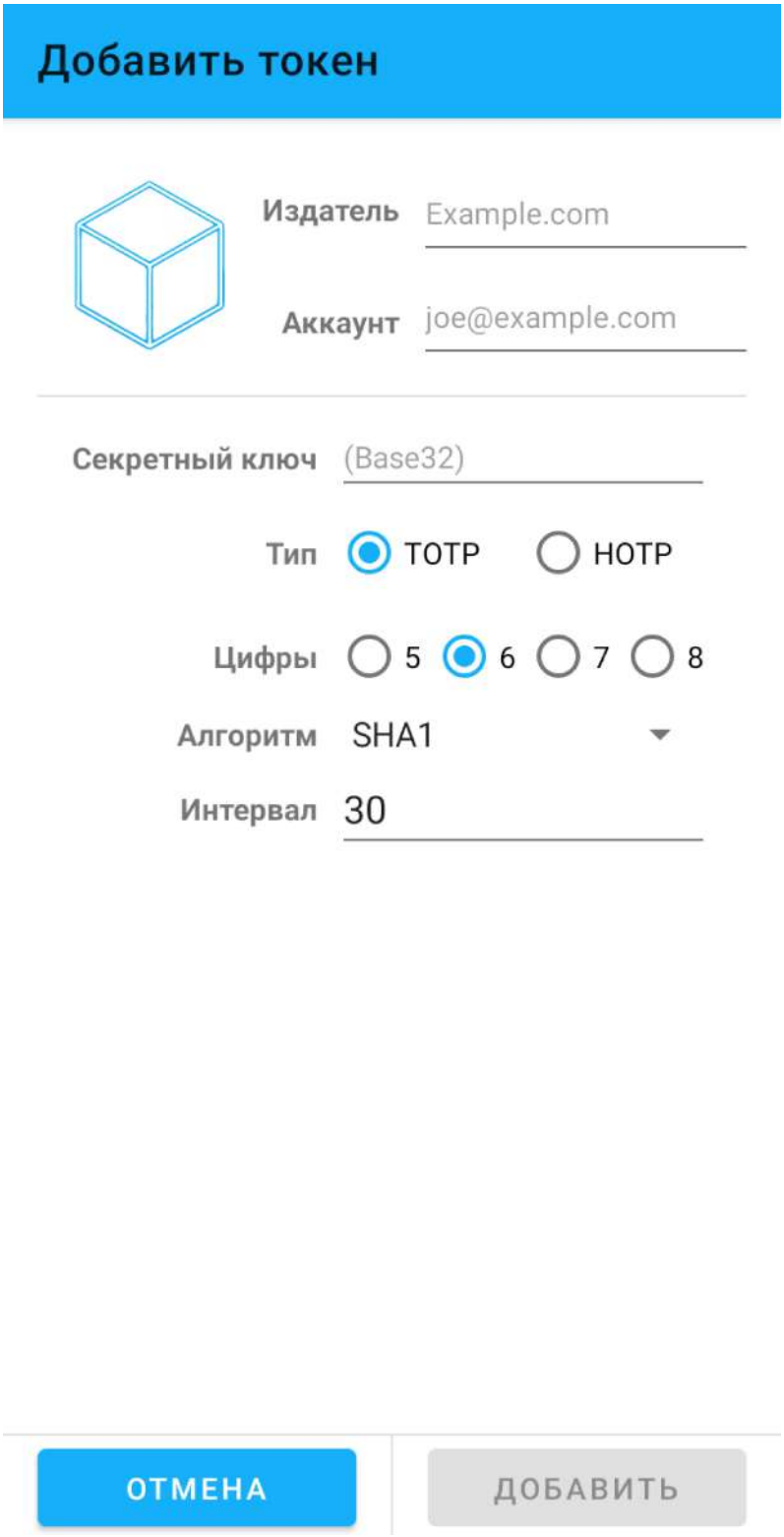


Копируем код, идем в приложение MEGA, нажимаем «Продолжить» внизу справа и вставляем код в появившееся поле. Двухфакторная аутентификация активирована.

Еще одно приложение, которое можно порекомендовать, это FreeOTP+. Оно не имеет дополнительных мер безопасности в виде шифрования паролем. [1] Однако, свою задачу выполняет хорошо.

Для того, чтобы добавить новую запись, нажимаем на три точки справа сверху и выбираем «Добавить токен».

В открывшемся окне, в графе «Издатель» вводим название сервиса, в графе «Аккаунт» ваш ник, а в графе «Секретный ключ», собственно, секретный ключ.



Нажимаем «Добавить». После этого в основном окне программы появится запись, где будут отображаться коды. Такова работа с данным приложением.

29 Пропускание трафика через Tor

Для анонимного Интернет-серфинга лучше использовать мобильную версию Tor-браузера. Существуют две версии приложения, одна с фиолетовым значком, другая с зеленым. Зеленый, это тестовая, а потому менее стабильная версия.[2] Посему рекомендую устанавливать браузер с фиолетовым значком.
[3]

Перед началом, сразу обращаю внимание, что для корректной работы Tor, необходимо, чтобы на устройстве были правильно выставлены время и дата. Поэтому, сначала настройте их. Это очень важно.

После установки открываем приложение, пропускаем все вступления и нажимаем на значок колеса сверху справа. Затем нажимаем «Конфигурация моста». Активируем «Использовать мост» и указываем «obfs4». Здесь уже непосредственно в программе забиты некоторые obfs-мосты, и мы можем не искать их отдельно. После этого возвращаемся в начало и нажимаем внизу «Соединиться». Если вдруг соединение не будет устанавливаться крайне продолжительное время, попробуйте вместо «obfs4» указать «snowflake», а если и это не сработает, то «meek-azure».

После того, как соединение установлено, нажимаем на три точки внизу справа и выбираем «Настройки», а затем «Настройки безопасности». Здесь указываем «Высший». Имейте ввиду, что многие сайты потеряют часть своего функционала, например, проигрывание видео. Поскольку здесь мы вынуждены работать без виртуализации, лучше перестраховаться и полностью отказаться от использования java-скриптов. На этом настройка Tor-браузера закончена.

Если по какой-то причине он будет работать некорректно, то можете попробовать другую его версию с зеленым значком.

Для пропускания через Tor трафика других приложений, нужна отдельная программа. Эта программа Orbot.[4] К сожалению, в последних версиях, она работает только в, так называемом, режиме VPN. То есть она использует VPN-подключение устройства, для пропускания трафика любых приложений через Tor. Если у вас есть root-права и вы используйте полноценный файервол, то в нем можете нужные приложения, активировать для VPN-соединения. Если же вы используйте NetGuard или Blokada, то вы не сможете активировать VPN-режим Orbot, оставив включенным файервол. Соответственно, придется использовать что-то одно. Я не рекомендую открывать возможность для потока трафика всех приложений. Здесь снова всплывает неполноценность мобильных

устройств. Тем не менее далее я покажу, как это приложение настроить и использовать.

После установки открываем его и для начала можно нажать на кнопку «Еще» внизу справа и выбрать «Настройки». Здесь нажимаем на «Исключенные узлы» и вбиваем маркировку страны вашего пребывания. Если находитесь в одной из стран СНГ, может все их маркировки и вбить, ru — Россия, ua — Украина, by — Белоруссия, kz — Казахстан и т.д. Также рекомендую активировать функцию «Изолировать адреса назначения». В этом случае трафик разных приложений будет перенаправляться через разные цепочки Tor. Также лучше отключить «Предпочитать IPv6 соединение».

После этого возвращаемся назад и нажимаем «Выбор приложений». Здесь отмечаем галочками те приложения, трафик которых хотим пропускать через Tor. Когда все настроено, нажимаем «Сохранить» вверху справа.

Далее нажимаем на «Подключить» внизу слева и нажимаем «Настроить подключение». Откроется окно с выбором типов подключения. Выбираем «Мост из Tor (Obfs4)». После чего нажимаем «Далее» внизу справа. Появится окно с капчей, поле под которой нужно заполнить, после чего нажать «Подключить» внизу справа. Появится сообщение о подключении к VPN. Имеется ввиду, что приложение активирует подключение устройства через Tor, используя настройку подключения VPN. Нажимаем «Запуск VPN». Если попытка подключения прошла неудачно, то выбираем «Snowflake (оригинал)». В этом случае, как правило проблем не возникает. Если же они все-таки возникнут, то выбираем «Пользовательский мост» и нажимаем «Далее» внизу справа. Откроется окно с предлагаемыми мостами. Но эти мосты работать не будут, если предыдущие подключения завершились неудачей. В этом случае можно в окне настройки подключения нажать «Запросить мост». Конфигурации мостов будут автоматически получены и добавлены в параметр пользовательского моста. После этого можно повторить подключение. Если это не помогло, нужно добавить мост полученный отдельно самостоятельно, например, можно попробовать перекинуть на устройство файл, в который вписаны конфигурации мостов, взятые с сайта проекта Tor, и скопировать в поле с конфигурациями мостов данные из файла.

Если подключение прошло нормально, трафик всех отмеченных приложений будет пропускаться через Tor. В этом случае Orbot запустит VPN-соединение на вашем устройстве. Если у вас есть root-права и вы используйте

полноценный файервол, то в нем можете нужные приложения, активировать для VPN-соединения. Если же вы используйте NetGuard или Blokada, то вы не сможете активировать VPN-режим Orbot, оставив включенным файервол. Соответственно, придется использовать что-то одно. Я не рекомендую открывать возможность для потока трафика всех приложений.

К сожалению, Orbot на многих устройствах, особенно старых и дешевых, работает очень нестабильно, и вам, возможно, вообще не удастся с его помощью пропустить трафик какого-либо приложения через Tor. Соединение просто не будет устанавливаться. В очередной раз мы приходим к тому, что смартфоны, это ущербная вещь. Заменить компьютер для полноценной приватной Интернет-активности они не способны. Несмотря на это, возможно у вас данный инструмент будет работать стабильно, и в таком случае, вам даже удастся осуществить относительно приватное общение. Об инструментах для этого общения я сейчас расскажу. Но прежде стоит разобраться с некоторыми популярными решениями, которые часто представляют, как свободные и этичные инструменты для общения.

30 Сомнительные свободные мессенджеры

Сейчас речь пойдет об инструментах, которые будучи свободными, имеют ряд проблем, не позволяющих считать их приемлемыми для использования.

Начнем мы с мессенджера Telegram. Клиент Telegram является свободным и даже доступен для скачивания в F-Droid. При этом, на странице Telegram на сайте F-Droid указано, что исходные коды данного мессенджера публикуются с опозданием, т.е. после выхода новой версии Telegram ее исходный коды выкладывается не сразу.[5] При этом программное обеспечение на серверах Telegram вовсе проприетарное. То есть, Telegram даже формально не является полностью свободным программным обеспечением.

Переписка в Telegram осуществляется без применения сквозного шифрования и хранится на серверах, что делает ее содержание доступным тому, кто контролирует эти сервера. Для сравнения, инструмент MEGA, о котором говорилось ранее, также хранит переписку на своих серверах, что позволяет обеспечивать синхронизацию между разными устройствами пользователя. Однако, на серверах она храниться в зашифрованном виде, — шифрование осуществляется непосредственно на устройстве пользователя, а потому содержимое остается недоступным владельцу сервера.

Помимо обычных чатов в Telegram имеются и секретные чаты, в которых переписка шифруется сквозным шифрованием и хранится непосредственно на устройствах пользователей. Сквозным шифрованием защищены и приватные звонки. Однако есть свидетельства, что при попытке осуществить зашифрованный звонок, он переключается на обычный. При этом отсутствует какая-либо маркировка — приватный звонок осуществляется или обычный.[6]

Кроме всего этого, Telegram привязывает аккаунты к номеру телефона, требуя его для регистрации в обязательном порядке. А это открывает дополнительные каналы атак, о чем уже говорилось ранее. Также он требует разрешения доступа к адресной книге и осуществляет функцию импорта контактов. Контакты импортируются на сервера, что открывает возможности для различных сливов, которые уже происходили.[7] В последних версиях Telegram внедрен функционал, позволяющий предотвратить слив своей адресной книги. Однако по-умолчанию этот функционал не включен.

В связи со всем сказанным, Telegram явно нельзя считать приемлемым инструментом для общения.

Следующим мессенджером с которым следует разобраться, это Signal. В отличии от Telegram, он является полностью свободным ПО и сквозное шифрование в нем применяется повсеместно. Несмотря на это, в репозиториях F-Droid его нет. В свое время некоторые энтузиасты использовали исходный код Signal для написания своих аналогов клиента. Однако разработчики оригинального Signal запретили разработчикам его независимых аналогов использовать его серверную часть, обращаться к их серверному ПО. Насколько я знаю, когда-то также были попытки поместить Signal в F-Droid, однако разработчики Signal потребовали удалить свое приложение из свободного магазина. Причина упорного избегания разработчиками Signal магазина F-Droid неизвестна.

Кроме всего этого, Signal также привязывает аккаунты своих пользователей к номеру телефона, со всеми вытекающими. И также практикует импорт контактов из адресной книги на сервера. Разработчики Signal пытаются успокоить пользователей, заявляя, что номера на сервера отправляются в хэшированном виде, однако из-за малого объема возможных хэшей, такая защита не очень устойчива к атаке полного перебора (брутфорсу).[8]

Таким образом, несмотря на то, что Signal выглядит пригляднее Telegram, в нем имеются весьма ощутимые проблемы, не позволяющие рекомендовать его

для использования.

Последний мессенджер, о котором хотелось бы здесь сказать, это Wire. Он, также как и Signal является полностью свободным ПО, как в своей клиентской, так и в серверной части. В отличии от Signal и Telegram, он не привязан к номеру телефона. Аккаунт можно привязать к телефону, но в качестве альтернативы присутствует возможность привязки к электронной почте, что все же куда более удачный вариант. Крайне смущает то, что несмотря на свободную лицензию, условия использования Wire имеют некоторые ограничения. Если вы на основе Wire захотите собрать свой собственный свободный мессенджер, то вы обязаны завязать его работу на сервера Wire.[9] Интересно, что Wire присутствует в репозиториях F-Droid, и на его странице в нем висит предупреждение о том, что оригинальный исходный код не является полностью свободным.[10] Таким образом, Wire является весьма сомнительной рекомендацией, хотя все же пригляднее Telegram или Signal.

Таков список известных мне сомнительных свободных средств для общения. К счастью существует довольно много достойных инструментов. О них мы и поговорим далее.

31 Инструменты для общения

Существуют различные федеративные инструменты для общения. В них сервер может поднять любой и нет какой-либо корпорации, которая бы все контролировала. Одним из таких инструментов является протокол XMPP. Чтобы общаться через него, используя какой-либо сервер, необходимо специальное приложение. Одним из таких клиентов является Conversation.[11] Через него можно осуществлять обмен сообщениями, файлами, местоположением, голосовую и видеосвязь, конференции, создание каналов. Поддерживает шифрование OpenPGP и OMEMO. Позволяет пропускать свой трафик через Tor, с помощью Orbot. Альтернативой ему может стать aTalk.[12] Его отличительной чертой является наличие, помимо шифрования OMEMO, также OTR. Если хотите использовать именно эту технологию, можете попробовать данное приложение.

Еще одним федеративным инструментом является протокол Matrix. Для общения с помощью него на мобильном устройстве существует много клиентов. Основным является приложение Element.[13] Позволяет обмениваться сообщениями, файлами, осуществлять голосовую и видеосвязь. Если это

приложение вас не устроит, то есть альтернативные клиенты, например SchildiChat[14] и Syphon.[15] Если Element откажется корректно работать, можете попробовать их.

Также существует приложение Status.[16] Данный инструмент не требует производить регистрации на каком-либо сервере. Нода выбирается самим клиентом из доступных. Также есть возможность вовсе отключить подключение к ноде, и общаться непосредственно между собеседниками, без использования какого-либо промежуточного узла. Мобильное приложение Status, помимо инструмента для общения, является также криптокошельком и Web3-браузером. Позволяет обмениваться сообщениями и файлами.

Существует еще один федеративный инструмент способный обеспечить стабильную связь. Это приложение Kontalk.[17] Позволяет обмениваться сообщениями, фотографиями, местоположением, создавать и обмениваться аудиозаписями. К сожалению, пока не реализован обмен любыми типами файлов, а также отсутствует аудио и видеосвязь. У этого инструмента есть еще один серьезный недостаток. Он привязан к номеру телефона, поэтому осуществлять анонимное общение через него не получится. Тем не менее, инструмент обеспечивает оконечное шифрование, не сканирует устройство и не передает на сервер данные адресной книги. Номер телефона для регистрации вы указывайте сами, а не приложение его считывает и использует. За счет этого, к одному аккаунту можно привязать несколько устройств, которые могут быть даже не связаны с тем, в котором непосредственно используется указанный номер телефона. Если вы неискушенный пользователь и вам очень нужна стабильная защищенная связь, пусть и не обеспечивающая высший уровень приватности, то Kontalk станет прекрасной заменой проприетарным мессенджерам.

Также существуют полностью децентрализованные средства связи, в которых общение осуществляется непосредственно между собеседниками, без использования промежуточного сервера.

Одним из них является протокол Tox. Существует функциональное, хорошо поддерживаемое приложение для общения по нему, TRIfa.[18] Альтернативой является клиент aTox.[19] В нем возможен только обмен сообщениями и файлами.

Также существует инструмент Jami.[20] К сожалению, Jami не всегда работает стабильно. Иногда наблюдается потеря связи с сетью, сообщения могут не доходить. Аудио и видеосвязь может идти с задержками. Файлы, особенно крупные, больше нескольких мегабайт, могут не передаваться. Несмотря на все это, Jami перспективный инструмент.

32 Общение с помощью Session

Наиболее стабильным приватным средством для общения является Session. В репозиториях F-Droid присутствует неофициальный клиент Session, с выпиленным несвободным кодом.[21] Дело в том, что в оригинальном Session присутствует функционал для взаимодействия с инструментами Google, позволяющими мгновенно получать уведомления о новых сообщениях. Этот функционал является несвободным. Ввиду сказанного рекомендую

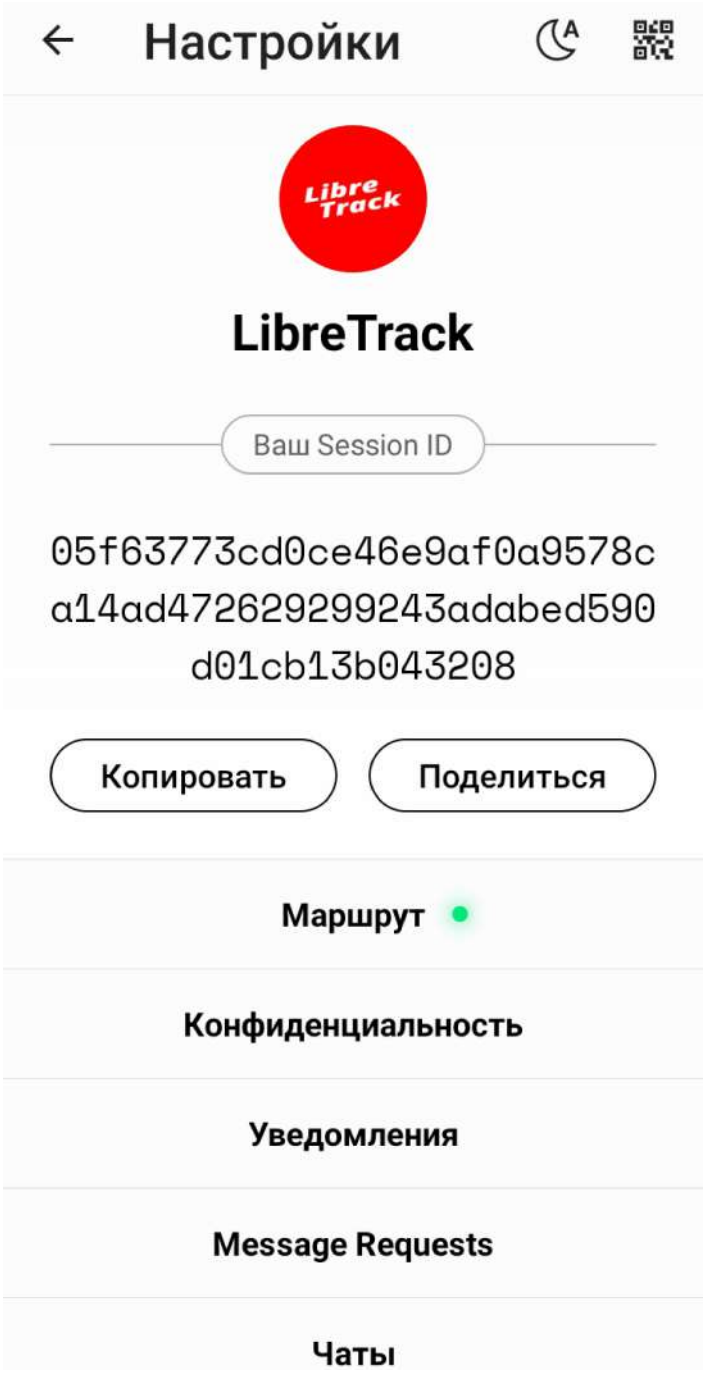
использовать именно эту версию клиента.

Устанавливаем и запускаем его. Если у вас уже есть аккаунт, то можете нажать «Восстановить Session ID». Затем необходимо ввести секретную фразу и ник. После этого откроется основное окно клиента.

Если аккаунта еще нет, то нажимаем «Создать Session ID». Высветится наш идентификатор, который лучше скопировать в менеджер паролей. После этого нажимаем «Продолжить». Вводим ник и нажимаем «Продолжить». Далее я рекомендую указать «Медленный режим», чтобы не связываться с сервисами Google.

Открывается основное окно программы. Нажимаем на кнопку «Продолжить» вверху слева, чтобы создать секретную фразу для восстановления аккаунта. Высветится секретная фраза, которую нужно скопировать в менеджер паролей. Она понадобится для переноса аккаунта на другое устройство. После этого снова возвращаемся в основное окно

программы. Если нажать на значок вверху слева, откроются настройки.

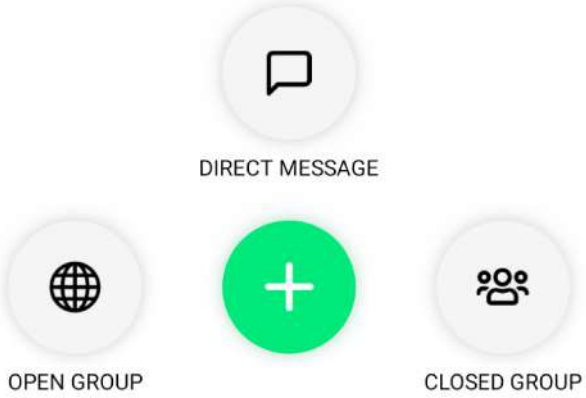


Здесь можно изменить ник и фото, увидеть и скопировать свой идентификатор. Во вкладке «Маршрут» отображается цепочка анонимизации с указанием ip и страны каждого узла. Во вкладке «Конфиденциальность», если хотите отправлять голосовые сообщения и осуществлять звонки, активируйте «Voice and video calls». Остальные настройки выставляете по своим потребностям. Во вкладке «Message Requests» отображаются запросы в контакты.

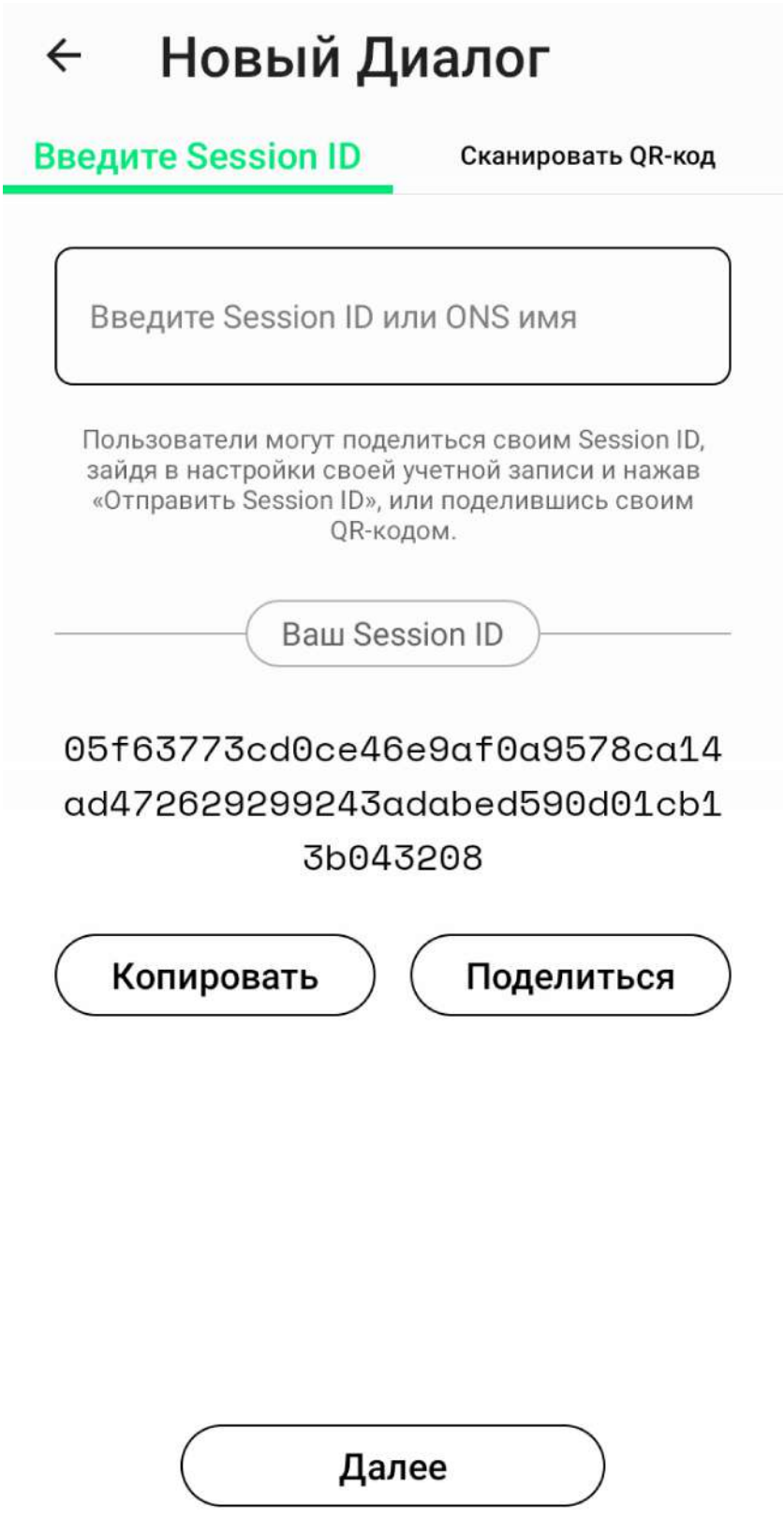
Чтобы добавить контакт, в основном окне нажимаем на зеленый значок «плюс».


AR
SESSION
У вас еще нет контактов
Начать Сессию

Затем выбираем «Direct Message».

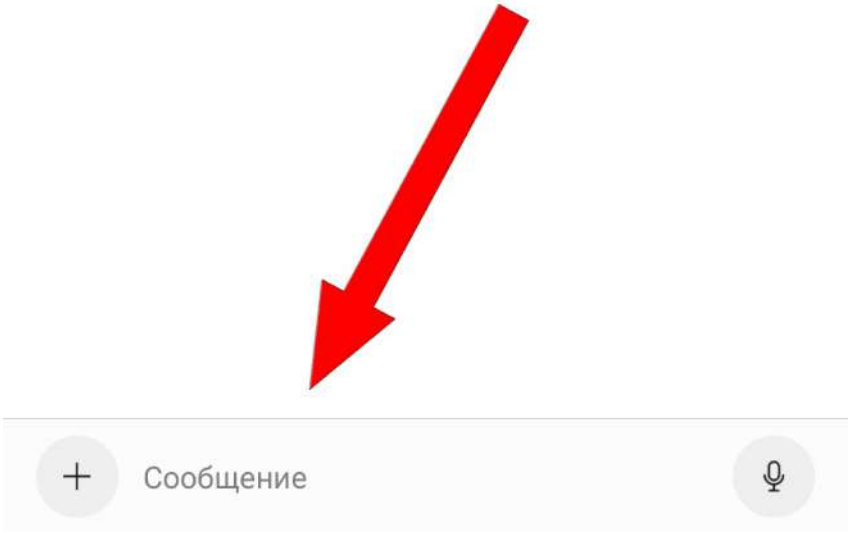


Здесь необходимо указать идентификатор собеседника или отсканировать QR-код и нажать «Далее».

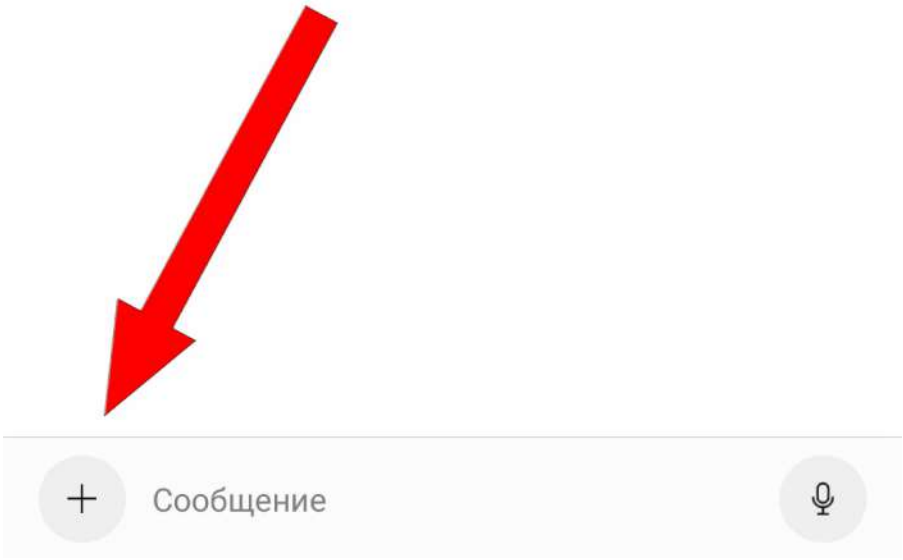


Откроется окно диалога и вы сможете отправить собеседнику сообщение. Вы не будите видеть его ник до тех пор, пока он вам не ответит и не примет в свои контакты. Чтобы написать сообщение, вводим его текст в поле внизу и

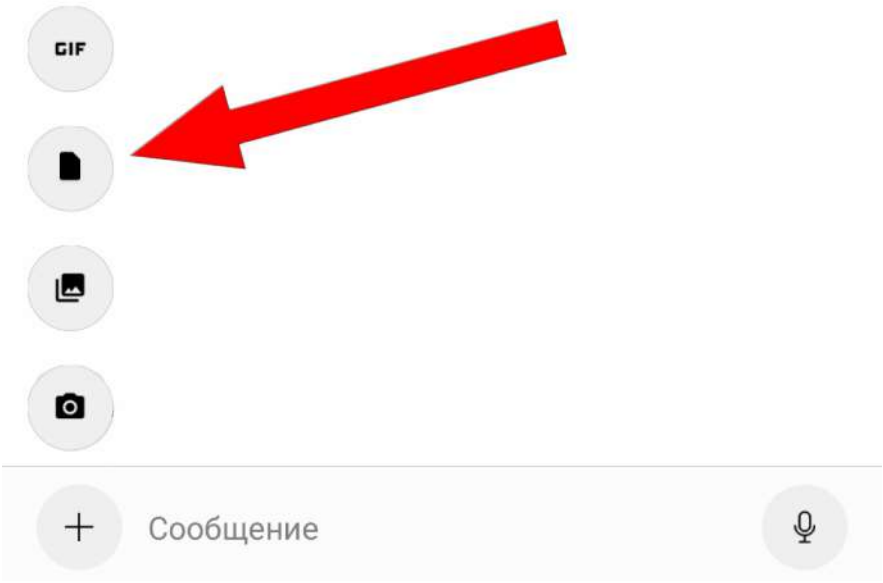
нажимаем значок самолетика справа.



Чтобы отправить файл, нажимаем на значок «плюс» слева от поля ввода.



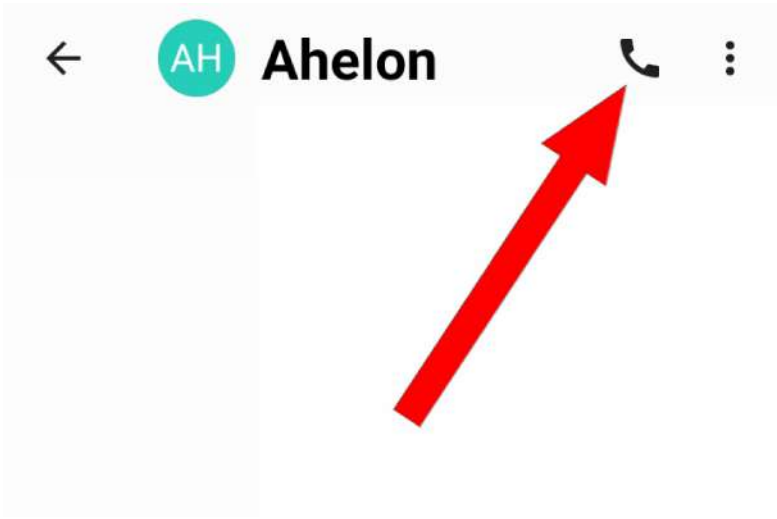
Затем нажимаем на значок файла.



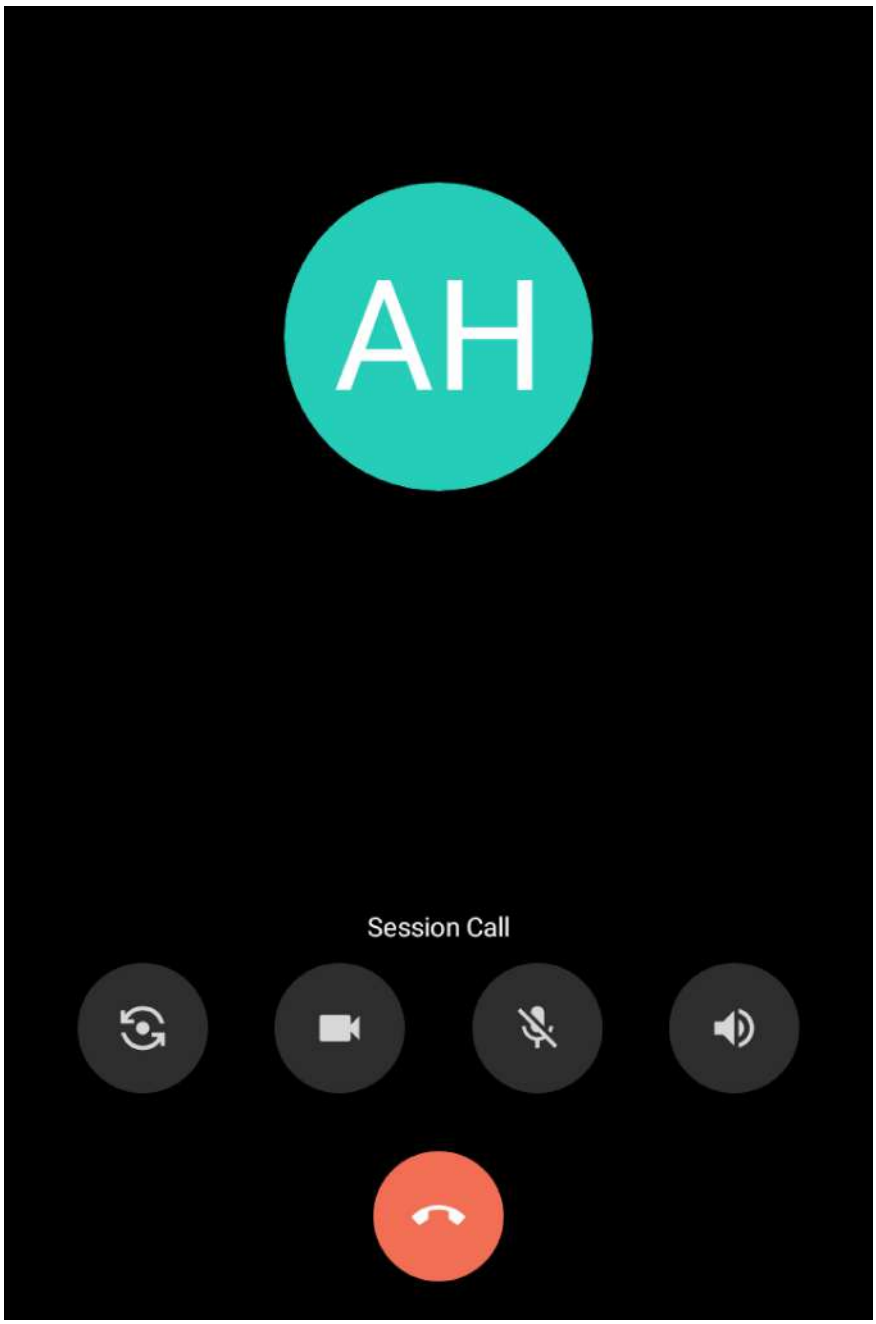
Выбираем нужный файл и отправляем.

Когда собеседник присылает вам фото или видеофайл, под ним появляется надпись «Нажмите, чтобы скачать медиа». При нажатии на нее, появляется сообщение, доверять ли контакту. При нажатии «Скачать», производится скачивание файла. При пересылке собеседником других типов файлов, при нажатии на них, вверху появляются варианты действий — переслать, сохранить или удалить. Для сохранения нужно нажать значок дискеты.

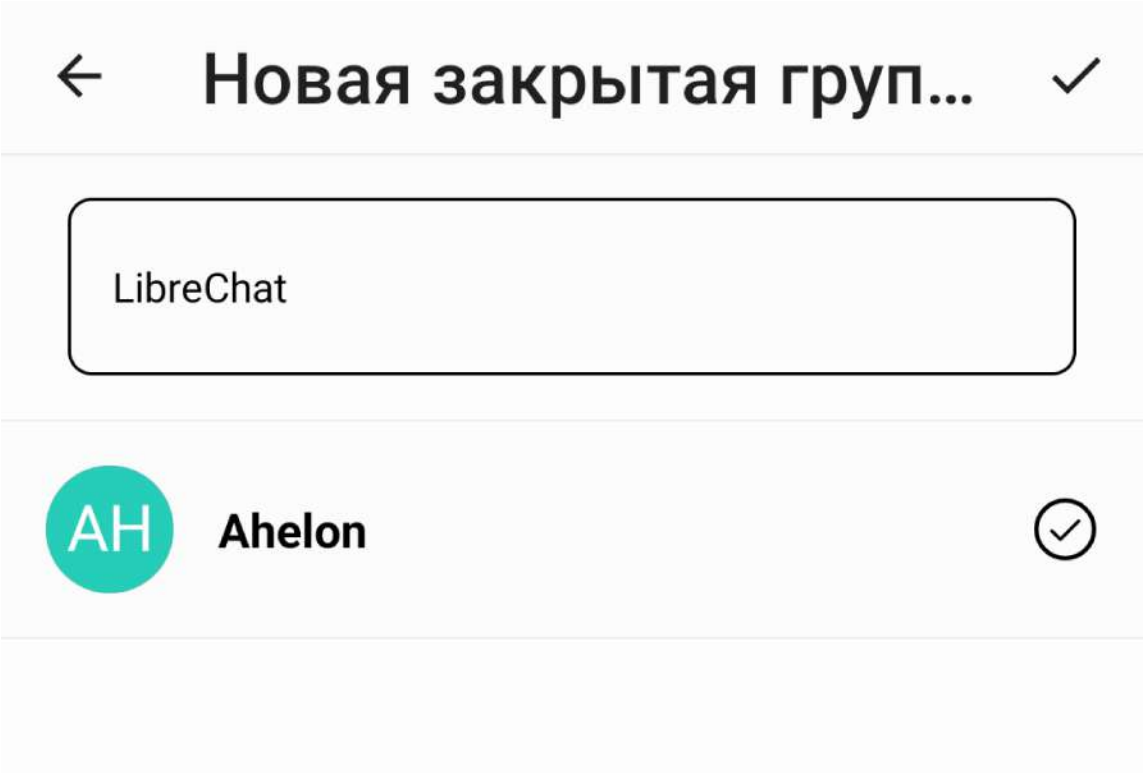
Чтобы совершить звонок, нажимаем на значок телефонной трубки вверху справа.



Если необходимо видео, его можно активировать во время звонка, нажав на значок камеры.

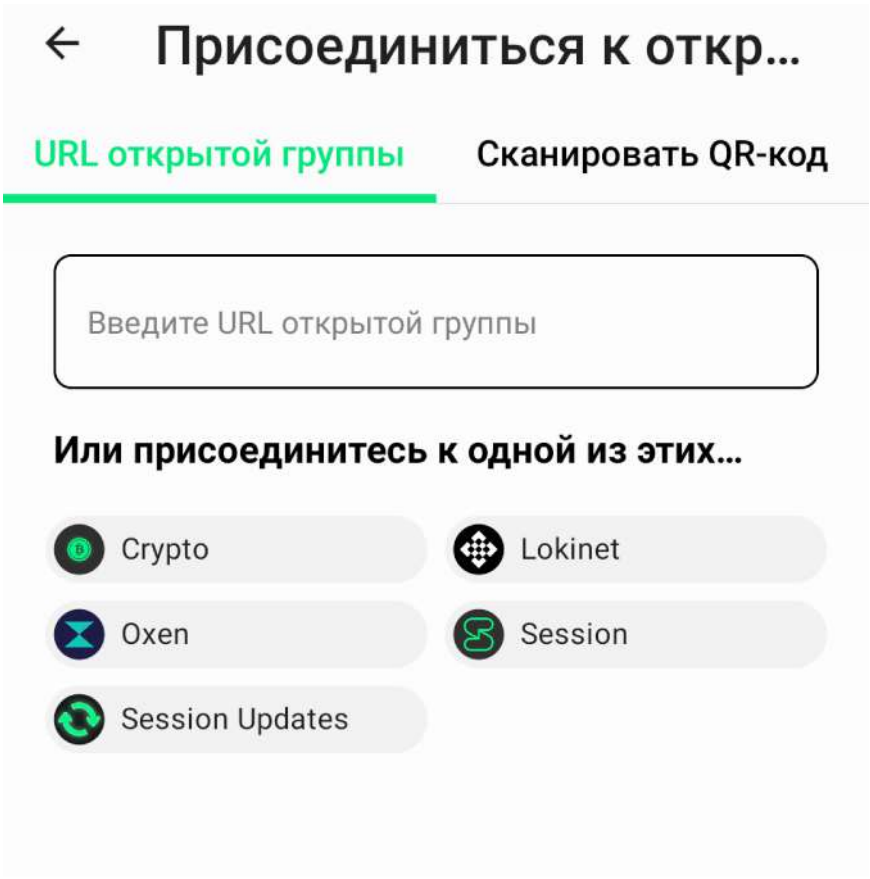


Чтобы создать закрытую группу, в основном окне также нажимаем на значок «плюс» и выбираем «Closed Group». Далее вводим название группы и отмечаем собеседников, которых хотим пригласить в нее, после чего нажимаем галочку справа вверху.



Общение в групповом чате, такое же как и в обычном, за исключением отсутствия возможности совершать звонки.

Чтобы присоединиться к открытой группе, также в основном окне нажимаем «плюс» и выбираем «Open Group». Далее вводим ссылку на группу или сканируем QR-код.



Такого общение в Session.

Если вдруг у вас возникнут проблемы с использованием этого приложения, можете попробовать оригинальный клиент. Для его установки необходимо подключить сторонние репозитории.[22]

Для добавления репозитория в F-Droid необходимо перейти в «Настройки» — это самая правая кнопка внизу, выбрать «Репозитории» и нажать на значок «плюс» вверху справа. В выскочившем окне необходимо ввести адрес репозитория

https://fdroid.getsession.org/fdroid/repo

И его отпечаток

DB0E5297EB65CC22D6BD93C869943BDCFCB6A07DC69A48A0DD8C7BA698EC04E6

После чего нажать «Добавить». Репозиторий будет добавлен. После чего список пакетов нужно обновить и можно скачивать клиент Session.

В целом работа в оригинальном клиенте такая же, как и в неофициальном.

33 Общение с помощью Mesh-технологий

Существуют инструменты, позволяющие осуществлять связь в отсутствие Интернета и мобильной сети. Mesh-технологии позволяют строить самостоятельные автономные распределенные сети, в которых устройства сообщаются через Wi-Fi или Bluetooth.[23] Такие сети могут функционировать в отсутствии глобальной сети, что может быть актуально для местностей с неразвитой инфраструктурой, в случае природных бедствий, когда сеть упала, или массовых волнений, когда ее отключили. Также это может быть актуально для построения защищенной изолированной сети в рамках отдельных организаций. Такая связь, ввиду ограничения используемых технологий, может осуществляться лишь на несколько десятков метров, непосредственно между двумя устройствами, однако, каждое в свою очередь может стать ретранслятором, позволяющим расширить зону охвата Mesh-сети.[24]

Одним из инструментов для такой связи является Serval Mesh.[25] Минусом данного приложения является отсутствие русскоязычного интерфейса.

Еще одним инструментом, поддерживающем помимо обмена сообщениями также аудио и видеосвязь, является Meshenger.[26] К сожалению, он также лишен русского интерфейса.

Также существует Fair Chat, который позволяет осуществлять связь только через Bluetooth.[27]

Отдельно необходимо отметить Briar.[28] Он поддерживает только обмен сообщениями, однако помимо Mesh-связи позволяет также общаться и через Интернет.

После установки и открытия приложения, необходимо ввести свой псевдоним, а затем пароль. Как обычно, создаем соответствующую запись в менеджере паролей. Далее нажимаем кнопку «Разрешить соединения» и разрешаем Briar работать в фоновом режиме. После чего нажимаем на «Создать учетную запись» внизу. Через несколько секунд запись будет создана и откроется основное окно приложения.

В Briar есть два способа добавления нового контакта. Один, если ваш собеседник находится рядом. Для его осуществления вам, соответственно, придется лично с ним встретиться. Второй, если собеседник далеко и нет возможности организовать с ним встречу.

В первом случае нажимаем на значок «плюс» внизу справа и выбираем «Добавить контакт поблизости». Появится пояснение, что такой способ позволит удостоверится, что вы общайтесь именно с тем человеком, с каким хотите, и никто не выдаст себя за него. Нажимаем «Продолжить». Даем разрешение на доступ приложению к камере, местоположению и Bluetooth. Вашему собеседнику необходимо проделать тоже самое. На экране появится вид камеры и QR-код. Вам необходимо взаимно сфотографировать QR друг друга. Для этого достаточно расположить код в поле зрения камеры, дальше приложение само все считает. Через некоторое время контакт будет добавлен.

Чтобы добавить собеседника, находящегося на расстоянии, нажимаем также на значок «плюс» внизу справа и выбираем «Добавить контакт на расстоянии». Откроется окно, где будет указана ссылка, которую необходимо отправить вашему собеседнику по отдельному каналу связи (обязательно защищенному). Здесь же находится поле, куда нужно ввести ссылку от вашего контакта. На следующем шаге нужно указать ник. После этого, контакт добавлен.

Чтобы начать общение, нажимаем на нужный контакт. Чтобы отправить сообщение вводим его текст в поле «Введите сообщение» внизу и нажимаем на значок бумажного самолетика справа от него. Вот и все, что необходимо для общения.

Помимо индивидуальных чатов в Briar можно создавать совместные, а также вести блоги.

Как уже было сказано, Briar способен осуществлять обмен сообщениями и через Интернет. Кроме того, это возможно делать через сеть Tor. Для этого в основном окне приложения нажимаем на три полоски вверху слева, в выскочившем поле выбираем «Настройки» и нажимаем на пункт «Подключение через Интернет». Выбираем «Использовать Tor с мостами».

Чтобы полностью закрыть приложение, в главном окне нажимаем на три полоски вверху слева и выбираем «Выход». Приложение будет закрыто и не будет висеть в фоне.

Как видно, Briar, это мессенджер, рассчитанный на максимальную приватность. Для тех, кому не нужен широкий функционал, но необходим действительно высокий уровень безопасности, он подойдет идеально. Это прекрасный инструмент.

---

1 Полное пособие по вычислительной свободе https://share.internxt.com/d/sh/file/329ff2c9358a0da0535f/8d5a8b6123e3182e0c5749cbb929d60862238fdece8ec125413821badd519776

2 О принципах работы сотовой сети можно почитать в Википедии https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B2%D1%8F%D0%B7%D1%8C. Более подробную информацию можно найти в статье Википедии о стандарте GSM https://ru.wikipedia.org/wiki/GSM

3 Об этом также сказано в этой статье Википедии https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B2%D1%8F%D0%B7%D1%8C. Также об этом можно почитать в этой статье Википедии https://ru.wikipedia.org/wiki/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BC%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C%D1%8E. Об этом же

1 рассказано в этой статье http://pro-gsm.info/location-update.html

2 Это указано в этой статье в Википедии https://ru.wikipedia.org/wiki/Location-based_service. Об этом же написано здесь https://web.archive.org/web/20100311073058/http://amobile.ru/info/phone/sensitivity.htm

3 На это указано здесь https://arendabs.ru/article/bazovaya-stantsiya-sotovoy-svyazi/. Также информацию можно найти в этой статье https://habr.com/ru/company/beeline/blog/194000/

4 На это указано здесь https://habr.com/ru/company/beeline/blog/194000/. Также сведения можно найти здесь http://rfdesign.ru/systems/cell.htm

5 О фемтосотах можно почитать в Википедии https://ru.wikipedia.org/wiki/%D0%A4%D0%B5%D0%BC%D1%82%D0%BE%D1%81%D0%BE%D1%82%D0%B0. Также они упомянуты здесь https://arendabs.ru/article/bazovaya-stantsiya-sotovoy-svyazi/

6 Об этом можно почитать в этой статье в Википедии https://ru.wikipedia.org/wiki/Location-based_service. Также об этом сказано здесь http://pro-gsm.info/location-tracking.html

7 На это указывается здесь http://pro-gsm.info/triangulation-legend.html. А также в этой статье https://www.mobile-review.com/articles/2009/triangulation.shtml

8 Это разбирается в данной статье http://pro-gsm.info/triangulation-legend.html. А также вот здесь https://www.mobile-review.com/articles/2009/triangulation.shtml

9 На это указывается здесь http://pro-gsm.info/location-tracking.html

10 Это объясняется здесь http://pro-gsm.info/google-maps-latitude.html

11 Об IMSI можно прочитать в Википедии https://ru.wikipedia.org/wiki/IMSI

12 Об этом сказано в той же статье в Википедии https://ru.wikipedia.org/wiki/IMSI

13 Об IMEI можно прочитать в Википедии https://ru.wikipedia.org/wiki/IMEI

14 О технологии Wi-Fi можно прочитать в Википедии https://ru.wikipedia.org/wiki/Wi-Fi. Существует свободное приложение для определения местоположения точек Wi-Fi https://f-droid.org/ru/packages/org.openbmap/index.html

15 Про технологию спутниковой навигации можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D1%83%D1%82%D0%BD%D0%B8%D0%BA%D0%B

1 E%D0%B2%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BD%D0%B0%D0%B2%D0%B8%D0%B3%D0%B0%D1%86%D0%B8%D0%B8

2 О GPS можно прочитать в Википедии https://ru.wikipedia.org/wiki/GPS

3 О ГЛОНАСС можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%93%D0%9B%D0%9E%D0%9D%D0%90%D0%A1%D0%A1

4 О системе «Галилео» можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BB%D0%B8%D0%BB%D0%B5%D0%BE_(%D1%81%D0%BF%D1%83%D1%82%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BD%D0%B0%D0%B2%D0%B8%D0%B3%D0%B0%D1%86%D0%B8%D0%B8)

5 О «Бэйдоу» можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%91%D1%8D%D0%B9%D0%B4%D0%BE%D1%83

6 Об этом сказано в этой статье https://slate.com/technology/2013/07/nsa-can-reportedly-track-cellphones-even-when-they-re-turned-off.html

7 Об этом можно узнать здесь http://www.a-rsb.ru/forum/lofiversion/index.php/t43.html

8 Сведения обо всем этом можно найти в комментариях здесь http://pro-gsm.info/spying-legend.html, сама статья разоблачает миф о прослушке выключенного телефона. Также в комментариях здесь https://users.livejournal.com/-adept-/47915.html#comments. И еще здесь https://habr.com/ru/post/112449/#comment_3636085

9 О нем можно прочитать здесь https://ru.wikipedia.org/wiki/%D0%A7%D0%B0%D1%81%D1%8B_%D1%80%D0%B5%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B2%D1%80%D0%B5%D0%BC%D0%B5%D0%BD%D0%B8

10 Сайт со стандартами сотовой связи https://www.3gpp.org/. Еще одним ресурсом о стандартизации является этот сайт https://www.etsi.org/standards

11 Об ОКС 7 можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%9E%D0%9A%D0%A1-7

12 Исследование на эту тему изложено здесь https://habr.com/ru/company/pt/blog/305472/

13 Это показано здесь https://habr.com/ru/company/pt/blog/283052/

случае сказано здесь https://habr.com/ru/company/pt/blog/328328/

2 На это указано здесь https://poisk-ru.ru/s13480t13.html

3 Обо всем этом сказано здесь https://www.osnews.com/story/27416/the-second-operating-system-hiding-in-every-mobile-phone/. Также об этом говорится здесь, к сожалению, без подтверждающих ссылок https://www.devever.net/~hl/nosecuresmartphone

4 Статья о cross-device tracking https://habr.com/ru/company/audiomania/blog/388701/. Статья с разбором технологии cross-device tracking https://xakep.ru/2017/05/04/uxdt/

5 Все это описано здесь https://techarks.ru/general/zashita/ultrazvukovoe-otslezhivanie-novaya-ugroza-kotoraya-otslezhivaet-ustrojstva-iot-s-ultrazvukovymi-signalami/

6 Статья, где предполагается возможность деанонимизации с помощью звуковых сигналов https://book.cyberyozh.com/ru/cross-device-tracking-deanonimizatsiya-polzovatelej-tor-vpn-proxy-pri-pomoschi-zvukovyih-mayachkov/. Еще одна статья о возможности деанонимизации https://www.pf.team/articles/zvukovye-maiachki---ugroza-anonimnosti__bmDHMhBF. Доклад о возможности деанонимизации https://media.ccc.de/v/33c3-8336-talking_behind_your_back

7 Статья, рассказывающая о полезности cross-device tracking для маркетологов https://habr.com/ru/company/dca/blog/283512/. Еще одна статья о маркетинговой полезности слежки и предлагающая услуги по ней https://www.byyd.me/ru/blog/2021/10/cross-device-targeting/

8 Исследование трекинга с помощью околоультразвуковых сигналов http://arstechnica.com/security/2013/12/scientist-developed-malware-covertly-jumps-air-gaps-using-inaudible-sound/. Еще одно исследование https://arstechnica.com/tech-policy/2015/11/beware-of-ads-that-use-inaudible-sound-to-link-your-phone-tv-tablet-and-pc/. И еще одно https://techcrunch.com/2014/07/24/silverpush-audio-beacons/. Дополнительную полезную информацию можно найти в комментариях здесь https://habr.com/ru/company/audiomania/blog/388701/comments/

9 Пример настройки колонок как микрофона https://siblimo.ru/kak-nastroit-kolonki-chtoby-oni-byli-mikrofonom/. Еще одна методика по использованию динамика как микрофона, где указывается, что необходим трансформатор для усиления сигнала https://trepuzec.ru/mozhno-li-ispolzovat-dinamiki-kak-

1 mikrofon/. Разъяснения по данному вопросу можно также найти здесь http://www.bolshoyvopros.ru/questions/1853878-mozhno-li-dinamik-ot-radio-ispolzovat-kak-mikrofon.html

2 Статья о вредоносной программе, незаметно меняющей назначения аудиоразъемов https://habr.com/ru/post/399363/

3 Об этом сказано в той же статье https://habr.com/ru/post/399363/

4 Обсуждение на эту тему можно найти здесь https://habr.com/ru/post/399363/comments/

5 Статья о возможности подслушивания через гироскоп смартфона https://tjournal.ru/tech/52031-gyroscope-sound-hack

6 Статья о деконволюции https://ru.bmstu.wiki/%D0%92%D0%BE%D1%81%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D1%8B%D1%85_%D1%81%D0%B8%D0%B3%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2

7 Статья о различных проблемах мобильного устройства https://habr.com/ru/post/410159/

8 Все это описано в этой статье https://habr.com/ru/post/575626/

9 Об этом можно почитать здесь https://mobile-review.com/all/articles/operator/laboratoriya-megafon-kakie-ustrojstva-horoshie-dlya-seti-operatora/

10 Страница Mudita Pure https://mudita.com/products/phones/mudita-pure/. О нем рассказано в этой статье https://habr.com/ru/company/selectel/blog/586844/. А также в этой https://www.opennet.ru/opennews/art.shtml?num=56134

11 Официальная страница Librem 5 https://puri.sm/products/librem-5/. О нем можно также почитать здесь https://losst.ru/purism-librem-5-smartfon-na-linux. О поддержке на нем системы GNU/Linux, Plasma Mobile сказано здесь https://puri.sm/posts/librem5-kde-partnership-announcement/, а о ее тестировании можно прочитать здесь https://www.opennet.ru/opennews/art.shtml?num=47202. О поддержке еще одной системы GNU/Linux, Ubuntu Touch сказано здесь https://puri.sm/posts/ubports-ubuntu-touch-on-librem5-collaboration/

12 Официальная страница Necuno Mobile https://necunos.com/community/. Также о нем можно прочитать здесь https://www.opennet.ru/opennews/art.shtml?num=49683

1 www.plasma-mobile.org/get/

2 Официальный сайт Ubuntu Touch https://ubports.com/. Также о ней можно прочитать в Википедии https://ru.wikipedia.org/wiki/Ubuntu_Touch. Список поддерживаемых устройств можно посмотреть здесь https://devices.ubuntu-touch.io/, не все указанные устройства полноценно поддерживаются.

3 Официальный сайт Replicant https://www.replicant.us/. Также о нем можно почитать в Википедии https://ru.wikipedia.org/wiki/Replicant

4 Список поддерживаемых устройств https://www.replicant.us/supported-devices.php

5 Официальный сайт LineageOS https://lineageos.org/. Также о ней можно прочитать в Википедии https://ru.wikipedia.org/wiki/LineageOS

6 Список поддерживаемых устройств https://wiki.lineageos.org/devices/

7 Официальный сайт Paranoid Android https://paranoidandroid.co/. Список поддерживаемых устройств https://paranoidandroid.co/downloads

8 Официальный сайт Omnirom https://omnirom.org/. Список поддерживаемых устройств https://omnirom.org/#devices

9 Официальный сайт /e/ https://e.foundation/. Список поддерживаемых устройств https://doc.e.foundation/devices/

10 О технологии NFC можно прочитать в Википедии https://ru.wikipedia.org/wiki/Near_Field_Communication

11 О заявлениях американских спецслужб о шпионаже ZTE и Huawei сказано в этой статье, при этом никаких доказательств, правда, не приводится https://tjournal.ru/tech/66283-glavy-cru-anb-i-fbr-posovetovali-amerikancam-otkazatsya-ot-smartfonov-huawei-i-zte. Опасения подтверждают японские гос. структуры https://www.vesti.ru/article/1421789, впрочем также бездоказательно. Проблемы с Huawei освещены в этой статье https://habr.com/ru/news/t/453560/. Указания на свидетельства шпионажа есть в этой статье https://akket.com/raznoe/149022-shpionazh-smartfonov-huawei-za-svoimi-vladeltsami-podtverdili-na-video.html, к сожалению без прямых ссылок. Huawei пыталось опровергать обвинения https://huawei.ru/news/5g-security/?sphrase_id=3255

12 Об универсальном бэкдоре в устройствах Xiaomi сказано здесь https://web.archive.org/web/20190424082647/http://blog.thijsbroenink.com/2016/09/xiaomis-analytics-app-reverse-engineered/. О слежке в устройстве можно прочитать здесь https://www.forbes.com/sites/thomasbrewster/2020/04/30/

1 exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/

2 Об этом сказано здесь https://ru-mi.com/blog/xiaomi-razblokirovka-zagruzchika.html

3 На это указано здесь https://androfon.ru/firmware-proshivka/razblokirovka-zagruzchika-motorola

4 О слежке в Motorola сказано здесь www.beneaththewaves.net/Projects/Motorola_Is_Listening.html. О подслушивании устройств сказано здесь https://web.archive.org/web/20170629175629/http://www.itproportal.com/2013/07/25/motorolas-new-x8-arm-chip-underpinning-the-always-on-future-of-android/

5 О необходимости регистрации в LG для разблокировки загрузчика сказано здесь https://4pda.biz/android-obshchee/3018-kak-razblokirovat-zagruzchik-lg-unlock-bootloader-lg.html. Кроме того, компания LG использует грязную политику в отношении пользователей своих телевизоров https://web.archive.org/web/20190917164647/http://openlgtv.org.ru/wiki/index.php/Achievements. О слежке через них сказано здесь https://www.techdirt.com/articles/20140511/17430627199/lg-will-take-smart-out-your-smart-tv-if-you-dont-agree-to-share-your-viewing-search-data-with-third-parties.shtml. А также здесь https://doctorbeet.blogspot.com/2013/11/lg-smart-tvs-logging-usb-filenames-and.html. О расширенном поле слежки сказано вот здесь https://rrrrambles.wordpress.com/2013/11/21/lg-tv-logging-filenames-from-network-folders/

6 О необходимости регистрации в HTC сказано здесь https://upgrade-android.ru/stati/stati/4724-razblokirovka-zagruzchika-htc.html

7 О необходимости слить личные данные Sony сказано здесь https://androidp1.ru/razblokirovat-bootloader-sony/. Известно также, что Sony не брезговало саботажем своей игровой приставки https://www.eff.org/deeplinks/2010/03/sony-steals-feature-from-your-playstation-3. Также эта компания выпускала и другие устройства с предустановленными лазейками https://www.vice.com/en/article/bj778v/sony-wants-to-sell-you-a-subscription-to-a-robot-dog-aibo-90s-pet. За ней также отмечено участие в сговоре по увеличению эксплуатации пользователей, о чем упомянуто здесь https://www.gnu.org/philosophy/copyright-versus-community.ru.html

8 На это указывает данная статья https://androfon.ru/firmware-proshivka/

1 razblokirovka-zagruzchika-samsung

2 О лазейке в Samsung говорится здесь https://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor. О еще одной говорится здесь https://www.theverge.com/circuitbreaker/2018/7/2/17528076/samsung-phones-text-rcs-update-messages. Еще об одной сказано здесь https://www.bleepingcomputer.com/news/security/sms-exploitable-bug-in-samsung-galaxy-phones-can-be-used-for-ransomware-attacks/. Также существует проблема с контролем программ пользователем https://www.bloomberg.com/news/articles/2019-01-08/samsung-phone-users-get-a-shock-they-can-t-delete-facebook. Эта проблема также описывается здесь https://arstechnica.com/gadgets/2015/07/samsung-sued-for-loading-devices-with-unremovable-crapware-in-china/

3 Об этом сказано здесь https://www.theguardian.com/technology/2018/oct/24/apple-samsung-fined-for-slowing-down-phones

4 Например, это показано здесь https://www.hardreset.info/ru/devices/lenovo/lenovo-zuk-z2-pro/faq/faq/bootloader-moto-unlock-lenovo-motorola-root/

5 Об установке Lenovo вредоносных программ сказано здесь https://www.computerworld.com/article/2984889/lenovo-collects-usage-data-on-thinkpad-thinkcentre-and-thinkstation-pcs.html

6 Официальный сайт TWRP https://twrp.me/. Также об этом рекавери можно почитать в Википедии https://ru.wikipedia.org/wiki/Team_Win_Recovery_Project

7 Для нужного устройства его можно скачать с официального сайта https://twrp.me/Devices/. Или поискать на этом сайте https://4pda.ru/

8 Программу Magisk Manager и пакет Magisk можно скачать по этой ссылке https://github.com/topjohnwu/Magisk/releases

9 Официальный сайт F-Droid https://f-droid.org/ru/. Также о нем можно почитать в Википедии https://ru.wikipedia.org/wiki/F-Droid

10 Скачать можно прямо с официального сайта https://f-droid.org/ru/

11 Страница G-Droid https://f-droid.org/ru/packages/org.gdroid.gdroid/

12 Страница M-Droid https://f-droid.org/ru/packages/com.mdroid/

13 Страница Foxy Droid https://f-droid.org/ru/packages/nya.kitsunyan.foxydroid/

14 Страница AnySoftKeyboard https://f-droid.org/ru/packages/com.menny.android.anysoftkeyboard/

15 Страница пакета русской локализации для AnySoftKeyboard https://f-

1 droid.org/ru/packages/com.anysoftkeyboard.languagepack.russian2/

2 Страница FFUpdater https://f-droid.org/ru/packages/de.marmaro.krt.ffupdater/

3 Страница Batch Uninstaller https://f-droid.org/ru/packages/com.saha.batchuninstaller/

4 Страница /system/app mover https://f-droid.org/ru/packages/de.j4velin.systemappmover/

5 Страница Amaze https://f-droid.org/ru/packages/com.amaze.filemanager/

6 Страница Activity Launcher https://f-droid.org/ru/packages/de.szalkowski.activitylauncher/

7 Страница App Manager https://f-droid.org/ru/packages/io.github.muntashirakon.AppManager/

8 Страница AFWall+ https://f-droid.org/ru/packages/dev.ukanth.ufirewall/

9 Об этом сказано в этой статье https://habr.com/ru/post/465945/, со ссылкой на эту страницу https://github.com/ukanth/afwall/issues/957

10 О технологии A-GPS можете почитать в Википедии https://ru.wikipedia.org/wiki/A-GPS

11 Страница NetGuard https://f-droid.org/ru/packages/eu.faircode.netguard

12 Страница Blokada https://f-droid.org/ru/packages/org.blokada.alarm/

13 Официальный сайт Simple Mobile Tools https://www.simplemobiletools.com/

14 Страница Simple Gallery https://f-droid.org/ru/packages/com.simplemobiletools.gallery.pro/

15 Страница Camera Roll https://f-droid.org/ru/packages/us.koller.cameraroll/

16 Страница Simple Camera https://f-droid.org/ru/packages/com.simplemobiletools.camera/

17 Страница Open Camera https://f-droid.org/ru/packages/net.sourceforge.opencamera/

18 Страница Simple Calendar https://f-droid.org/ru/packages/com.simplemobiletools.calendar.pro

19 Страница Simple File Manager https://f-droid.org/ru/packages/com.simplemobiletools.filemanager.pro/

20 Страница Dir https://f-droid.org/ru/packages/com.veniosg.dir/

21 Страница Simple Flashlight https://f-droid.org/ru/packages/com.simplemobiletools.flashlight

22 Страница Simple Music Player https://f-droid.org/ru/packages/com.simplemobiletools.musicplayer

1 ch.blinkenlights.android.vanilla/

2 Страница Simple Draw https://f-droid.org/ru/packages/com.simplemobiletools.draw.pro

3 Страница Markers https://f-droid.org/ru/packages/org.dsandler.apps.markers

4 Страница Simple Calculator https://f-droid.org/ru/packages/com.simplemobiletools.calculator/

5 Страница Simple Clock https://f-droid.org/ru/packages/com.simplemobiletools.clock/

6 Страница Fairphone Clock Widget https://f-droid.org/ru/packages/community.fairphone.clock/

7 Страница Voice Recorder https://f-droid.org/ru/packages/com.simplemobiletools.voicerecorder/

8 Страница Audio Recorder https://f-droid.org/ru/packages/com.github.axet.audiorecorder

9 Страница Call recorder for Android https://f-droid.org/ru/packages/com.callrecorder.android/

10 Страница Simple Dialer https://f-droid.org/ru/packages/com.simplemobiletools.dialer/

11 Страница Simple Contacts https://f-droid.org/ru/packages/com.simplemobiletools.contacts.pro/

12 Страница Simple SMS Messenger https://f-droid.org/ru/packages/com.simplemobiletools.smsmessenger/

13 Страница Simle Notes https://f-droid.org/ru/packages/com.simplemobiletools.notes.pro/

14 Страница Editor https://f-droid.org/ru/packages/org.billthefarmer.editor/

15 Страница SNotepad https://f-droid.org/ru/packages/info.aario.snotepad/

16 Страница VLC https://f-droid.org/ru/packages/org.videolan.vlc/

17 Страница LibreOffice https://f-droid.org/ru/packages/org.documentfoundation.libreoffice/

18 Страница Librera Reader https://f-droid.org/ru/packages/com.foobnix.pro.pdf.reader/

19 Страница MuPDF mini https://f-droid.org/ru/packages/com.artifex.mupdf.mini.app/

20 Страница Barcode Scanner https://f-droid.org/ru/packages/com.google.zxing.client.android/

1 com.example.barcodescanner/

2 Страница Binary Eye https://f-droid.org/ru/packages/de.markusfisch.android.binaryeye/

3 Страница SecScanQR https://f-droid.org/ru/packages/de.t_dankworth.secscanqr/

4 Страница WhatExp https://f-droid.org/ru/packages/fr.ludo1520.whatexp/

5 Страница Matrix Calc https://f-droid.org/ru/packages/com.alexkang.x3matrixcalculator/

6 Страница AnotherMonitor https://f-droid.org/ru/packages/org.anothermonitor/

7 Страница ScreenCam https://f-droid.org/ru/packages/com.orpheusdroid.screenrecorder/

8 Страница Squeez https://f-droid.org/ru/packages/csci567.squeez/

9 Страница DictionaryForMIDs https://f-droid.org/ru/packages/de.kugihan.dictionaryformids.hmi_android/

10 Страница Video Transcoder https://f-droid.org/ru/packages/protect.videoeditor/

11 Страница LTE Cleaner https://f-droid.org/ru/packages/theredspy15.ltecleanerfoss/

12 Страница PilferShush Jammer https://f-droid.org/ru/packages/cityfreqs.com.pilfershushjammer/

13 Страница SimpleTextCrypt https://f-droid.org/ru/packages/com.aidinhut.simpletextcrypt/

14 Страница Encrypt Text https://f-droid.org/ru/packages/dk.meznik.jan.encrypttext/

15 Страница Note Crypt Pro https://f-droid.org/ru/packages/com.notecryptpro/

16 Страница SealNote https://f-droid.org/ru/packages/com.twistedplane.sealnote/

17 Страница EDS Lite https://f-droid.org/ru/packages/com.sovworks.edslite/

18 Страница OpenKeychain https://f-droid.org/ru/packages/org.sufficientlysecure.keychain/

19 Страница Oversec https://f-droid.org/ru/packages/io.oversec.one/

20 Страница Elementary https://f-droid.org/ru/packages/com.ultramegatech.ey/

21 Страница Calcvac https://f-droid.org/ru/packages/de.drhoffmannsoftware.calcvac/

22 Об этом сказано здесь https://pingvinus.ru/news/2676. Более подробно это описано здесь https://habr.com/ru/company/itsumma/news/t/505782/

23 Разъяснения разработчиков https://brave.com/referral-codes-in-suggested-

1 sites/

2 Это описано здесь https://3dnews.ru/1033119/v-brave-obnarugen-bag-izza-kotorogo-brauzer-ostavlyaet-dannie-onionsaytov-v-trafike-dns. Подробнее рассказано здесь https://www.block-chain24.com/news/novosti-bezopasnosti/brave-uzhe-neskolko-mesyacev-teryaet-dannye-bezopasno-li-ispolzovat

3 Это показано в видео https://www.youtube.com/watch?v=trkUyrYObVQ

4 Это показано в том же видео https://www.youtube.com/watch?v=trkUyrYObVQ

5 Страница со списком шифрующих DNS-серверов https://dnscrypt.info/public-servers/

6 Сайт Vivaldi https://vivaldi.com/ru/

7 Статья с объяснением отличий Vivaldi от Chromium https://vivaldi.com/blog/vivaldi-browser-vs-google-chrome/

8 Статья о поддержке Vivaldi блокировщиков рекламы https://habr.com/en/company/vivaldi/blog/456048/. Статья о новом способе отслеживания пользователей, внедряемом Google и отказе его использования Vivaldi https://habr.com/en/company/vivaldi/blog/552408/

9 Статья о том, как Google препятствует распространению Vivaldi https://habr.com/en/post/406461/

10 Статья с разъяснением политики публикации исходного кода и лицензирования Vivaldi https://habr.com/en/company/vivaldi/blog/526300/. Страница с разъяснениями открытости Vivaldi https://jon.vivaldi.net/a-few-words-about-open-source-vivaldi/

11 Политика конфиденциальности Vivaldi https://vivaldi.com/ru/privacy/browser/

12 Страница Privacy Browser https://f-droid.org/ru/packages/com.stoutner.privacybrowser.standard/

13 Страница K9 Mail https://f-droid.org/ru/packages/com.fsck.k9/

14 Страница FairEmail https://f-droid.org/ru/packages/eu.faircode.email/

15 Страница SimpleEmail https://f-droid.org/ru/packages/org.dystopia.email/

16 Страница Pretty Easy Privacy https://f-droid.org/ru/packages/security.pEp/

17 Страница Delta Chat https://f-droid.org/ru/packages/com.b44t.messenger/

18 Страница Tutanota https://f-droid.org/ru/packages/de.tutao.tutanota/

19 Страница KeePassDX https://f-droid.org/ru/packages/com.kunzisoft.keepass.libre/

1 menion.android.whereyougo/

2 Страница OsmAnd https://f-droid.org/ru/packages/net.osmand.plus/

3 Страница Trekarta https://f-droid.org/ru/packages/mobi.maptrek/

4 Страница pMetro https://f-droid.org/ru/packages/com.utyf.pmetro/

5 Страница Transporter https://f-droid.org/ru/packages/de.grobox.liberario/

6 Страница LibreSpeed https://f-droid.org/ru/packages/com.dosse.speedtest/

7 Страница Forecastie https://f-droid.org/ru/packages/cz.martykan.forecastie/

8 Страница Simple Weather https://f-droid.org/ru/packages/com.a5corp.weather/

9 Страница Good Weather https://f-droid.org/ru/packages/org.asdtm.goodweather/

10 Страница Weater https://f-droid.org/ru/packages/org.secuso.privacyfriendlyweather/

11 Официальный сайт OpenWeatherMap https://openweathermap.org/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/OpenWeatherMap

12 Страница LibreTranslater https://f-droid.org/ru/packages/de.beowulf.libretranslater/

13 Сайт LibreTranslate https://libretranslate.com/

14 Страница Linphone https://f-droid.org/ru/packages/org.linphone/

15 Страница Lumicall https://f-droid.org/ru/packages/org.lumicall.android/

16 Страница Mumla https://f-droid.org/ru/packages/se.lublin.mumla/

17 Страница Plumble https://f-droid.org/ru/packages/com.morlunk.mumbleclient/

18 Страница Jitsi Meet https://f-droid.org/ru/packages/org.jitsi.meet/

19 Страница AndStatus https://f-droid.org/ru/packages/org.andstatus.app/

20 Страница Twitlatte https://f-droid.org/ru/packages/com.github.moko256.twitlatte/

21 Страница Frost for Facebook https://f-droid.org/ru/packages/com.pitchedapps.frost/

22 Страница SlimSocial for Facebook https://f-droid.org/ru/packages/it.rignanese.leo.slimfacebook/

23 Страница MaterialFBook https://f-droid.org/ru/packages/me.zeeroooo.materialfb/

24 Страница Face Slim https://f-droid.org/ru/packages/org.indywidualni.fblite/

25 Страница Tinfoil for Facebook https://f-droid.org/ru/packages/com.danvelazco.fbwrapper/

1 me.jakelane.wrapperforfacebook/

2 Страница SlimSocial for Twitter https://f-droid.org/ru/packages/it.rignanese.leo.slimtwitter/

3 Страница Tifoil for Twitter https://f-droid.org/ru/packages/com.mill_e.twitterwrapper/

4 Страница Barinsta

5 Страница Easy Repost https://f-droid.org/ru/packages/net.schueller.instarepost/

6 Страница NewPipe https://f-droid.org/ru/packages/org.schabi.newpipe/

7 Страница WebTube https://f-droid.org/ru/packages/cz.martykan.webtube/

8 Страница YouTube Stream https://f-droid.org/ru/packages/org.thiolliere.youtubestream/

9 Страница YaShlang https://f-droid.org/ru/packages/su.sadrobot.yashlang/

10 Страница мобильного приложения MEGA https://play.google.com/store/apps/details?id=mega.privacy.android.app&referrer=meganzmobileapps

11 Страница Aurora Store https://f-droid.org/ru/packages/com.aurora.store/

12 О многофакторной аутентификации можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B3%D0%BE%D1%84%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%BD%D0%B0%D1%8F_%D0%B0%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F

13 О принципах работы двухфакторной аутентификации сказано в этой статье https://habr.com/ru/company/1cloud/blog/277901/

14 О технологии аутентификации по времени можно прочитать в Википедии https://ru.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm. Об аутентификации по событию также есть статья https://ru.wikipedia.org/wiki/HOTP

15 Сравнительная оценка двухфакторной аутентификации через SMS и приложение дана здесь https://www.securitylab.ru/blog/personal/bezmaly/351101.php. О проблемах двухфакторной аутентификации можно прочитать здесь https://apptractor.ru/info/articles/haos-dvuhfaktornoy-autentifikatsii.html

16 О проблемах метода аутентификации через SMS можно прочитать здесь https://oddstyle.ru/wordpress-2/stati-wordpress/pochemu-dvuxfaktornaya-autentifikaciya-ne-vsegda-garantiruet-zashhitu.html

17 Страница Aegis https://f-droid.org/ru/packages/com.beemdevelopment.aegis/

1 org.liberty.android.freeotpplus/

2 Страница тестовой версии Tor Browser for Android https://guardianproject.info/apps/org.torproject.torbrowser_alpha/

3 Страница Tor Browser for Android https://guardianproject.info/apps/org.torproject.torbrowser/

4 Страница Orbot https://guardianproject.info/apps/org.torproject.android/

5 Страница Telegram на сайте F-Droid https://f-droid.org/ru/packages/org.telegram.messenger/

6 Об этих проблемах сказано на странице проекта Whonix https://www.whonix.org/wiki/Telegram

7 Утечка базы данных пользователей Telegram https://www.gazeta.ru/tech/2020/06/24_a_13129027.shtml

8 О проблемах Signal сказано здесь https://cryptoworld.su/na-skolko-bezopasen-signal-messendzher/. А также здесь https://www.whonix.org/wiki/Signal

9 Об этом сказано здесь https://github.com/wireapp/wire-desktop/blob/dev/LICENSE. А также здесь https://github.com/wireapp/wire-ios/blob/develop/README.md

10 Страница Wire на сайте F-Droid

11 Страница Conversations https://f-droid.org/ru/packages/eu.siacs.conversations/

12 Страница aTalk https://f-droid.org/ru/packages/org.atalk.android/

13 Страница Element https://f-droid.org/ru/packages/im.vector.app/

14 Страница SchildiChat https://f-droid.org/ru/packages/de.spiritcroc.riotx/

15 Страница Syphon https://f-droid.org/ru/packages/org.tether.tether/

16 Страница Status https://f-droid.org/ru/packages/im.status.ethereum/

17 Страница Kontalk https://f-droid.org/ru/packages/org.kontalk/

18 Страница TRIfa https://f-droid.org/ru/packages/com.zoffcc.applications.trifa/

19 Страница aTox https://f-droid.org/ru/packages/ltd.evilcorp.atox/

20 Страница Jami https://f-droid.org/ru/packages/cx.ring

21 Страница неофициального клиента Session https://f-droid.org/ru/packages/network.loki.messenger.fdroid/

22 Страница с указанием репозиториев Session https://fdroid.getsession.org/

23 О Mesh-сетях можно прочитать в Википедии https://ru.wikipedia.org/wiki/Mesh-%D1%81%D0%B5%D1%82%D1%8C

24 Об этом можно прочитать здесь https://ru.wikipedia.org/wiki/Cjdns

25 Страница Serval Mesh https://f-droid.org/ru/packages/org.servalproject/