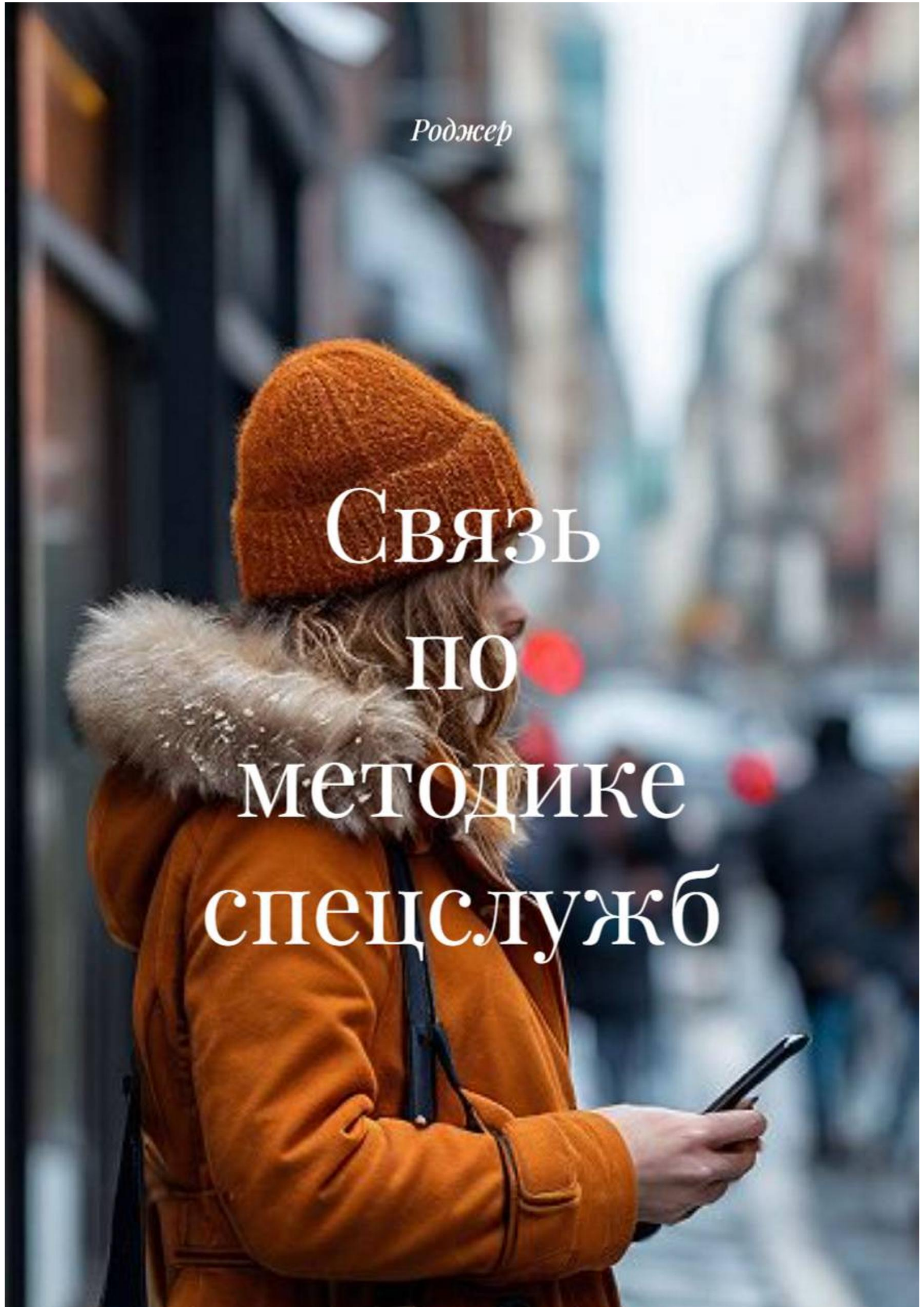
Роджер



Связь по методике спецслужб

Роджер

Связь по методике спецслужб

«Автор»
2026

Роджер

Связь по методике спецслужб / Роджер — «Автор», 2026

Вы каждый день совершаете одно и то же действие, сами того не замечая: достаёте телефон, открываете мессенджер с гордой надписью «безопасно» и отправляете сообщение. «Привет», «Как дела?», «Встретимся завтра». И вы искренне верите, что это — частный акт, маленькая тайна, доступная лишь вам и вашему собеседнику.На самом деле вы только что сделали публичное заявление. Не перед одним-двумя людьми, а перед десятком невидимых свидетелей. Ваш провайдер, сотовый оператор, сервер мессенджера, системы государственного мониторинга и даже иностранные спецслужбы — все они не просто услышали, а записали, заархивировали и привязали этот факт к вашей личности на годы вперёд. И им не нужно читать ваш текст. Им достаточно метаданных: кому, когда, откуда и как часто вы пишете. Этой информации хватило спецслужбам, чтобы уничтожить целые ячейки, не прочитав ни одного слова.

Содержание

Роджер
Связь по методике спецслужб

Глава 1: Конец анонимности и смерть наивности

(Ландшафт угроз: кто, как и зачем тебя слушает)

Ты достаёшь телефон, разблокируешь экран, открываешь мессенджер, тот самый, в который ты веришь, потому что на нём написано «безопасно», «шифрованно» или даже «независимо». Ты печатаешь короткое сообщение. «Привет». «Как дела?». «Встретимся завтра в восемь». Ты нажимаешь «отправить», откладываешь телефон в сторону и чувствуешь лёгкое удовлетворение — ты только что совершил частный, личный, безопасный акт коммуникации.

Ты ошибаешься, катастрофически. Ты только что совершил не приватный акт, а публичное заявление в присутствии десятка невидимых свидетелей, которые не просто услышали, а записали, протоколировали, заархивировали и привязали к твоей личности.

Давай назовём их поимённо.

Первое звено: Твой интернет-провайдер. Каждый пакет данных, который покидает твой телефон, сначала проходит через его оборудование. Он знает, когда ты вышел в сеть, сколько трафика отправил, какие протоколы использовал. Он может не знать точное содержание сообщения (если оно зашифровано), но он знает факт: ты, с твоего IP-адреса, в такое-то время, связался с таким-то сервером. Этого достаточно для базового профилирования.

Второе звено: Твой сотовый оператор. Он видит ещё больше. Он знает, к какой вышке сотовой связи ты был привязан в момент отправки, знает твою геолокацию с точностью до дома. Он знает, как часто и в какое время суток ты обмениваешься данными. Он хранит эти записи — не один день, а годы, как того требуют законы многих стран.

Третье звено: Сервер мессенджера. Даже если мессенджер использует сквозное шифрование, сервер всё равно является точкой маршрутизации. Он видит метаданные: кто написал, кому, когда, с какого устройства, с какой геолокации, какой объём данных был передан, использовалась ли камера, включался ли микрофон. Эти метаданные часто более ценны, чем само сообщение.

Четвёртое звено: Межсетевой экран твоей страны. Это не просто «сетевой фильтр». Это система глубокого анализа пакетов — Deep Packet Inspection, она не просто смотрит на заголовки пакетов, она заглядывает внутрь, ищет ключевые слова, маркеры подозрительного трафика, паттерны поведения. Если твоё сообщение содержит что-то из «стоп-листа», оно будет автоматически помечено и отправлено в дополнительную обработку.

Пятое звено: Правительственные системы мониторинга. В каждой крупной стране есть такой институт. В России — СОРМ (Система оперативно-розыскных мероприятий). В США — PRISM и XKeyscore. В Китае — Золотой щит. В Великобритании — Tempora. Они не просто слушают. Они записывают всё, что проходит через магистральные каналы связи и они хранят это годами, на случай, если ты когда-нибудь станешь интересен.

Шестое звено: Иностранные спецслужбы. Если ты достаточно интересен, либо просто если ты когда-нибудь окажешься в зоне пересечения интересов, к твоим данным могут получить доступ АНБ, ЦРУ, ФСБ, Моссад, БНД, MI6 и ещё десяток разведывательных служб. Они работают не по законам твоей страны. Они работают по своим правилам, они не спрашивают разрешения.

Все они, каждое из этих звеньев, делают одну и ту же вещь, не просто читают. Они записывают, навсегда, твоё сообщение не исчезнет, оно станет частью логов, архивов, баз данных, которые хранятся в дата-центрах по всему миру. Через десять лет ты сможешь не вспомнить, что писал в тот вечер, но система помнит и она никогда не забывает.

Добро пожаловать в реальность. Анонимность умерла примерно в 2013 году.

Это был переломный год. Парень по имени Эдвард Сноуден, бывший подрядчик АНБ, вышел из тени с несколькими терабайтами секретных документов. Он показал миру, что АНБ собирает метаданные всех телефонных звонков в США и большей части мира, что программа PRISM имеет прямой доступ к серверам Google, Facebook, Apple, Microsoft и других гигантов, что агентства способны заходить в камеры мобильных телефонов, слушать микрофоны, читать сообщения в реальном времени. Мир ахнул, потом привык, потом сделал вид, что ничего не произошло.

Похороны анонимности затянулись, до сих пор находятся люди, которые верят в «исчезающие сообщения» в Telegram. Которые думают, что VPN делает их невидимыми в сети, которые уверены, что их никто не слушает, потому что они «никому не интересны».

Эта книга — не для них. Эта книга для тех, кто уже перестал прятать голову в песок, для тех, кто понял простую истину: если ты не управляешь своей связью, связь управляет тобой. Мы будем говорить на языке оперативников — жёстко, цинично, без иллюзий, без сладких обещаний «абсолютной безопасности». Ты узнаешь, как работают реальные протоколы скрытой коммуникации, как минимизировать свои цифровые следы, как не попадать в ловушки, которые расставляют алгоритмы и системы слежки. Не для того, чтобы стать шпионом, для того, чтобы перестать быть прозрачной мишенью.

Три уровня угрозы: Кто именно охотится на твои данные

Прежде чем начать защищаться, нужно понять, от кого ты защищаешься. В цифровой разведке принято выделять три уровня противников, они отличаются по возможностям, по инструментам и по целям. Твоя защита должна быть адекватна самому сильному из тех, кто реально тобой интересуется.

Первый уровень: Массовый сбор данных — рекламные сети и алгоритмы

Это уличные попрошайки, они не охотятся лично на тебя, они собирают дань со всех прохожих, которые проходят мимо них. Google, Meta (организация признана экстремистской и запрещена на территории Российской Федерации), TikTok, Amazon, Яндекс, VK — все эти корпорации построили свою бизнес-модель на сборе данных. Чем больше они знают о тебе — тем точнее могут таргетировать рекламу, тем выше их доходы.

Что они собирают? Всё, до чего могут дотянуться, твои поисковые запросы, геолокационные данные, покупки, лайки, подписки, время, которое ты проводишь в приложениях, контакты в твоей адресной книге, список приложений на телефоне, твои разговоры — да, технически «для улучшения голосового ассистента», они слушают твой микрофон, читают твою почту, анализируют твои фотографии, строят на тебя профиль, который точнее, чем ты сам можешь себя описать.

Им не нужно расшифровывать твой секретный чат. Им достаточно знать метаданные: что ты в 2:14 ночи 32 минуты переписывался с контактом, который географически находится в той же квартире, что и ты, алгоритм мгновенно вычислит, что у тебя роман. Он сделает это быстрее, чем ты сам осознаешь глубину своих чувств, и он начнёт показывать тебе рекламу свадебных платьев, цветов, ресторанов и отбеливателей для зубов, потому что алгоритм «знает», что ты скоро понадобишься рекламодателям.

Второй уровень: Государственный мониторинг — системы вроде СОРМ, PRISM и XKeyscore

Это уже не попрошайки с протянутой рукой. Это патруль с дубинками. Они действуют не для продажи тебе товаров, а для контроля и обеспечения безопасности, как они это понимают.

У каждого уважающего себя государства есть система тотального перехвата трафика. В России это СОРМ — Система оперативно-розыскных мероприятий, которая по закону обязана быть установлена на всех узлах связи. В США это PRISM и XKeyscore, которые собирают данные напрямую с магистральных каналов интернета. В Китае — это Великий файрвол и Золотой щит, которые не только фильтруют контент, но и сканируют весь проходящий трафик. В Европе — это системы, работающие под эгидой национальных служб и обмена данными в рамках «Пяти глаз».

Они не просто слушают, они записывают всё, что проходит через магистральные каналы. Они хранят это годами. Их задача — не прочитать твой секрет прямо сейчас. Их задача — иметь возможность поднять архив за любой день, если ты вдруг станешь интересен по какой-то причине. Ты можешь быть серой мышью десять лет, но на одиннадцатый год ты написал что-то не то, попал в список, пересекся с нежелательным лицом или просто был в неправильное время в неправильном месте и твой цифровой скелет достанут из шкафа. Метаданные не умирают, они ждут.

Третий уровень: Таргетное наблюдение — ты сам являешься целью

Это уже спецназ, он приходит не за всеми, приходит лично за тобой. Если ты журналист-расследователь, оппозиционный активист, бизнесмен с опасными конкурентами, свидетель преступления, бывший сотрудник спецслужб, человек, обладающий компроматом, — ты цель. Ты не просто «данные в массе». Ты — конкретный объект, за которым ведётся целенаправленная охота.

Против тебя работают профессионалы, они не будут ждать, пока ты сам сольёшь данные в сеть. Они установят тебе на телефон шпионское ПО — через фишинговую ссылку, через поддельное обновление, через взломанное приложение, поднимут твои передвижения по биллингу сотовых вышек за последние полгода, прослушают твою квартиру через лазерный микрофон, направленный на оконное стекло, будут использовать IMSI-перехватчики, чтобы отслеживать твой телефон даже в офлайн-режиме.

На этом уровне защита мессенджера не имеет значения. Если устройство скомпрометировано — если на нём стоит шпионское ПО — ты можешь шифровать сообщения хоть собственным кодом, изобретённым лично тобой. Злоумышленник всё равно читает их на твоём экране до того, как они ушли в сеть. Ты можешь использовать самый безопасный мессенджер в мире, но если твой телефон «заражён», всё, что ты видишь, видит и он.

Кто ты на этой шахматной доске?

Прежде чем ты продолжишь читать, тебе нужно честно ответить себе на один вопрос: кто твой враг?

Потому что защита от разных уровней требует разных мер, абсолютной защиты не существует, есть только адекватность угрозе. Если ты защищаешься от рекламных сетей, тебе достаточно базовой цифровой гигиены: отключить лишние разрешения, поставить блокировщик рекламы, использовать приватные настройки в приложениях. Если ты защищаешься от государства, тебе придётся менять образ жизни: отказываться от смартфона в пользу одноразовых кнопочных аппаратов, купленных за наличку; пользоваться общественным Wi-Fi только через VPN с правом на неведение; минимизировать свои цифровые следы. Если ты цель таргетного наблюдения — никакая книга не сможет тебе помочь. Тебе нужен личный специалист по оперативной безопасности, полная смена легенды, возможно — переезд в другую страну.

Ответь себе честно: кто твой враг? От этого зависит всё, что ты будешь делать дальше.

Что такое метаданные и почему твоё сообщение неважно

Ты думаешь, что главное в сообщении — это его содержание. Текст, смысл, слова. «Я люблю тебя». «Завтра в 12:00». «Номер счёта 40817...». Это самая распространённая ошибка. Ты думаешь, что, если зашифруешь текст — ты в безопасности. На самом деле текст неважен. Текст — это только письмо, а письмо всегда идёт в конверте.

Метаданные — это конверт, они гораздо важнее письма.

Что именно скрыто в метаданных твоей коммуникации?

Кто с кем общается. Не содержание сообщения, а сам факт связи. Ты написал этому конкретному человеку, этот факт уже зафиксирован.

Когда. Точное время отправки, дата, продолжительность — если речь о звонке или видео-сессии.

Откуда. Твой IP-адрес, геолокация, идентификатор вышки сотовой связи, к которой ты был привязан, то есть спецслужбы или алгоритмы знают не только что ты сказал, но и где ты находился, когда это говорил.

Тип коммуникации. Звонок, текстовое сообщение, файл, стикер, голосовое. По одному этому признаку можно многое понять о характере общения.

Устройство. Модель телефона, версия операционной системы, уникальные идентификаторы устройства, которые невозможно сменить без полной замены телефона.

Этой информации достаточно, чтобы уничтожить человека, не прочитав ни одного его слова.

Реальный кейс: в 2013 году АНБ официально признало, что использует метаданные телефонных звонков для выявления террористических сетей, они не читали СМС, не слушали разговоры. Они строили граф связей между людьми, используя только метаданные. Алгоритм анализировал цепочки звонков, временные разрывы между звонками, общие контакты, географическое распределение и на основе этих данных — без единого расшифрованного сообщения — спецслужбы уничтожали целые ячейки. Содержание сообщений было не нужно. Метаданных оказалось достаточно.

Вывод: если ты хочешь сохранить приватность, недостаточно зашифровать текст. Нужно спрятать сам факт связи. Нужно скрыть, что ты с кем-то разговариваешь. Это — задача принципиально другого уровня сложности.

Принцип оперативной связи: прячься на виду

В разведке существует принцип, которому сотни лет. Если хочешь спрятать дерево — посади его в лесу. Если хочешь спрятать сообщение — отправь его там, где миллиарды таких же сообщений отправляются каждую секунду, никто не анализирует весь поток. Ресурсы аналитиков ограничены — на всех не хватит вычислительных мощностей и человеческого внимания.

Именно поэтому спящие агенты часто ведут безобидные блоги о вязании, кулинарии, футболе, а шахматные серверы считаются идеальным местом для передачи кодов — нотации шахматных партий легко читаются как зашифрованные сообщения, но никто не подозревает это, потому что вокруг миллионы других партий. Именно поэтому твоя безобидная книга, проданная тиражом 12 экземпляров на Amazon, может содержать ключи для резидента в Тегеране. Потому что никто не читает книги неизвестных авторов, никто не смотрит стримы с тремя зрителями, не анализирует нотацию шахматной партии двух любителей с рейтингом 800.

Шум — твой союзник, массовость — твоё укрытие, публичность — твоя анонимность, чем больше ты похож на «нормального» пользователя, тем меньше вероятность, что тебя заметят. Чем более банальны твои цифровые привычки, тем выше шанс, что ты останешься невидимым.

Прежде чем двигаться дальше — прежде чем изучать мессенджеры, настраивать VPN, думать о смене легенды — ты должен провести разведку на себя, понять, какую информацию о тебе уже собрал мир, это упражнение займёт около часа, оно отрезвляет, показывает, насколько ты прозрачен для тех, кто хочет тебя видеть.

Шаг первый: Google-досье на самого себя. Открой браузер в режиме инкогнито (чтобы поисковая выдача не подстраивалась под твои прошлые запросы). Введи свои полные ФИО в кавычках — «Иванов Иван Иванович», потом номер телефона в разных форматах — с

кодом страны, без кода, через дефис, затем адрес электронной почты, старый никнейм, который ты использовал в юности. Просмотри результаты, ты удивишься, сколько информации о тебе уже есть в открытом доступе — и сколько из неё ты сам выложил когда-то по наивности.

Шаг второй: Геолокационные метаданные. Зайди в Google Хронологию (если у тебя аккаунт Google) или аналогичный сервис у Apple. Посмотри, где ты был три года назад во вторник в 14:30, увидишь маршрут своего передвижения с точностью до дома. Это — то, что знает корпорация, а значит, может узнать и тот, кто получит доступ к твоему аккаунту. Если тебе не нравится, что кто-то знает, где ты был, — отключай эти функции, но помни: отключение не означает, что данные удалены, они просто перестают быть доступными тебе в этом интерфейсе.

Шаг третий: Аудит мессенджеров. Открой настройки конфиденциальности в каждом мессенджере, который ты используешь — Telegram, WhatsApp, Signal, Viber. Проверь: кто видит твой номер телефона? Кто видит твоё фото профиля? Кто видит время твоего последнего входа в сеть? Включи всё, что можно выключить, поставь режим «никто» или «мои контакты» везде, где это возможно. Это не сделает тебя невидимым, но создаст лишние барьеры для случайного сбора данных.

Шаг четвёртый: Проверка утечек паролей. Зайди на сайт Have I Been Pwned. Введи свою электронную почту, увидишь список утечек, в которых засветился твой аккаунт. Если там есть пароли, которые ты до сих пор используешь, — смени их немедленно. Если ты используешь один и тот же пароль на нескольких сайтах, прекрати это делать. Каждая новая утечка делает тебя более уязвимым.

Шаг пятый: Цифровой след в соцсетях. Пройдись по своим постам за последние 5-7 лет, посмотри, что ты публиковал. Есть ли там информация о твоём месте работы, адресе, родственниках, привычках, перемещениях? Если есть — подумай, стоит ли оставлять это в открытом доступе. Удали всё, что может быть использовано против тебя или хотя бы скрой настройки приватности.

Глава 2: Великий мессенджер-обман

(Сравнительный анализ: кто, где и как хранит твои секреты)

Ты провёл аудит, знаешь теперь, что твой цифровой след уходит в прошлое на годы, что метаданные текут рекой, которую не перекрыть простым «я ничего не скрываю». Ты хочешь защититься, открываешь магазин приложений — и видишь десятки мессенджеров, каждый из которых обещает тебе вечную любовь, абсолютную безопасность и неприкосновенность твоей переписки. «Сквозное шифрование» — написано на одном. «Исчезающие сообщения» — на другом. «Мы не читаем ваши чаты, мы не храним ваши данные, мы заботимся о вашей приватности» — это общий рефрен.

Звучит как музыка, на деле — это маркетинговая колыбельная, под которую ты засыпаешь, пока твои данные перетекают на серверы, разбросанные по юрисдикциям, где само понятие «приватность» — это не более чем анекдот, который рассказывают за ужином, когда никто не слушает.

Сегодня мы разберём мессенджеры так, как их разбирает оперативный аналитик, готовящий канал связи для полевого агента. Без рекламных буклетов, без красивых обещаний, без доверия к словам разработчиков. Только факты, архитектура, пять критериев, которые позволяют отличить реальную защиту от маркетинговой мишуры.

Пять критериев оценки: что смотреть под капотом, а не на блестящую обёртку

Прежде чем мы начнём разбирать конкретные приложения, нужно договориться о системе координат, любой мессенджер можно оценить по пяти ключевым параметрам. Каждый из них — это отдельная точка уязвимости или защищённости, ни один идеальный мессенджер не существует. Всегда есть компромисс, задача — выбрать тот, где компромиссы минимальны и соответствуют твоему профилю угрозы.

Первый критерий: Сквозное шифрование — E 2 EE , End - to - End Encryption .

Это базовая, минимальная защита, сквозное шифрование означает, что сообщение шифруется на твоём устройстве и расшифровывается только на устройстве получателя. Сервер, через который проходит сообщение, видит лишь белый шум — хаотичный набор байтов, не имеющий смысла без ключа расшифровки. Если в мессенджере нет E2EE, или оно отключено по умолчанию, или действует только для «секретных» режимов, а не для всех чатов — считай, что ты отправляешь открытки, их читает почтальон, читает начальник почты, читает тот парень, который подкупил сортировщика, твой текст доступен всем, кто имеет доступ к серверу.

Второй критерий: Метаданные.

Даже при идеально работающем сквозном шифровании сервер всё равно знает, кому ты пишешь, когда ты пишешь, откуда ты пишешь, как часто ты пишешь и с какого устройства. Эта информация называется метаданными, она часто более ценна, чем само сообщение. Хороший мессенджер минимизирует сбор метаданных, идеальный — не собирает их вовсе, но таких почти нет. Вопрос в том, сколько именно сервер знает о тебе и твоих контактах.

Третий критерий: Юрисдикция.

Где зарегистрирована компания, владеющая мессенджером? Где физически расположены серверы? Какие законы действуют в этой стране? Швейцария и Объединённые Арабские Эмираты — это две разные галактики в плане приватности. Сервер в США подпадает под действие Cloud Act — закона, который позволяет американским спецслужбам запрашивать данные у компаний даже в том случае, если данные хранятся за пределами США. Сервер в России — под действие СОРМ и «пакета Яровой», которые обязывают операторов связи хранить дан-

ные и предоставлять доступ к ним по первому требованию. Сервер в Китае — под действие Закона о кибербезопасности, который требует от компаний сотрудничать с государственными органами и хранить данные внутри страны.

Четвёртый критерий: Привязка к номеру телефона.

Номер телефона — это твой цифровой паспорт, он привязан к твоему удостоверению личности, которое ты предъявлял в салоне связи, когда оформлял SIM-карту. Если мессенджер требует номер телефона для регистрации, он автоматически связывает твою «анонимную» переписку с твоей реальной личностью. Спецслужбам, имеющим доступ к базам сотовых операторов, не нужно вычислять тебя — ты сам предоставил им ключ к идентификации.

Пятый критерий: Открытость кода.

Является ли код мессенджера открытым? Может ли независимый специалист проверить, что программа делает на самом деле? Если код закрыт, ты вынужден верить разработчику на слово. В разведке на слово не верят даже маме, открытый код позволяет аудиторам, исследователям и просто энтузиастам проверять наличие закладок, корректность реализации шифрования, минимизацию сбора данных. Открытый код — это не гарантия, но это минимальное условие для доверия.

Теперь, когда система координат определена, мы можем пройтись по основным мессенджерам, которые есть на рынке, посмотреть, что они предлагают на самом деле — не в рекламных проспектах, а в реальности.

Telegram :

Telegram — это, пожалуй, самый коварный из всех, он не выглядит как угроза, он красивый, быстрый, удобный, с миллионами стикеров, каналов, ботов. Он создан Павлом Дуровым, который публично говорит о свободе и независимости, кажется воплощением приватности, но это иллюзия.

Telegram — это социальная сеть с функцией мессенджера, а не безопасный мессенджер. Запомни это раз и навсегда. Все обычные чаты — те, в которых ты общаешься каждый день со своими друзьями, коллегами, родственниками — хранятся на серверах Telegram в расшифрованном виде. Это означает, что Telegram владеет ключами, что компания может прочитать твою переписку в любой момент — по запросу спецслужб, по решению акционеров, по ошибке администратора или по техническому сбою.

Есть секретные чаты — они используют сквозное шифрование, но они неудобны: не синхронизируются между устройствами, доступны только с того телефона, на котором созданы, и о них постоянно забывают. Большинство пользователей Telegram даже не знают об их существовании. Метаданные собираются в огромных объёмах. Юрисдикция мессенджера — ОАЭ, куда Дуров перенёс штаб-квартиру. Формально это «независимость», но аналитики задаются вопросом: насколько независимой может быть компания, работающая в стране, где законы о кибербезопасности строги, а отношения со спецслужбами не подлежат раскрытию?

Telegram блокировался в России в 2018–2020 годах — его пытались заблокировать, и хотя блокировка была технически сложной и неполной, факт остаётся фактом. В Иране Telegram блокировали многократно. В Китае он запрещён полностью. Использование Telegram через VPN в авторитарных странах — это не защита, сигнал, красный флаг, который говорит системе мониторинга: «Я что-то скрываю, обратите на меня внимание».

WhatsApp :

WhatsApp — самый популярный мессенджер в мире и самый опасный с точки зрения приватности, не потому что его шифрование плохое — оно как раз хорошее. WhatsApp использует протокол Signal для шифрования контента. Это значит, что текст твоего сообщения не прочитает никто, кроме тебя и получателя, но это единственная хорошая новость.

WhatsApp принадлежит Meta (организация признана экстремистской и запрещена на территории Российской Федерации) — компании, которая была признана экстремистской в

России и которая построила свой бизнес на сборе данных. Все метаданные — кто, кому, когда, откуда, с какого устройства — льются в материнскую компанию. Meta (организация признана экстремистской и запрещена на территории Российской Федерации) использует эти данные для таргетинга рекламы, для построения теневых профилей, для связывания твоей активности в WhatsApp с твоей активностью в Instagram (организация признана экстремистской и запрещена на территории Российской Федерации) и Facebook (организация признана экстремистской и запрещена на территории Российской Федерации). Даже если ты не пользуешься другими продуктами Meta (организация признана экстремистской и запрещена на территории Российской Федерации), компания знает, что ты существуешь и знает, с кем ты общаешься.

В Китае WhatsApp запрещён. В Объединённых Арабских Эмиратах запрещены голосовые и видеозвонки через WhatsApp. В Иране и Северной Корее — полный запрет. В России WhatsApp пока не трогают массово, но с учётом того, что он принадлежит Meta (организация признана экстремистской и запрещена на территории Российской Федерации), и с учётом развития системы СОРМ-3, которая теоретически может перехватывать трафик даже зашифрованных каналов, ситуация может измениться в любой момент.

Signal :

Signal — это лучший общедоступный мессенджер для обычного человека, который действительно хочет приватности. Это почти золотой стандарт. Почему?

Во-первых, сквозное шифрование включено по умолчанию для всех чатов, никаких секретных режимов — всё защищено с первого сообщения.

Во-вторых, минимизация метаданных. Signal собирает только самую необходимую информацию — время последнего входа в сеть, факт регистрации, и всё. Технология Sealed Sender скрывает даже факт того, кто именно отправил сообщение, это значит, что сервер знает, что сообщение было отправлено, но не знает, кем именно.

В-третьих, открытый код. Любой может проверить, что Signal делает с твоими данными, это проверяется регулярно независимыми аудиторами.

В-четвёртых, некоммерческая организация. Signal не принадлежит корпорациям, заинтересованным в сборе данных.

Есть одна фатальная дыра, которая делает Signal непригодным для тех, кто действительно скрывается от государства. Это привязка к номеру телефона, твой идентификатор в Signal — это твой мобильный номер. Если ты скрываешься от режима, который контролирует сотовых операторов, твой аккаунт в Signal автоматически засвечен. Спецслужбы видят, что этот номер зарегистрирован в Signal, хотя они не видят, что ты пишешь, они видят факт использования, а факта использования достаточно, чтобы привлечь внимание.

В 2024 году Signal был заблокирован в России. В Иране и Китае он также под запретом. Само наличие приложения Signal на твоём телефоне при досмотре — это компромат. Это сигнал: «Я что-то скрываю, и я выбрал для этого самый защищённый инструмент». Иногда это даже более подозрительно, чем использование Telegram.

Конец ознакомительного фрагмента.