

Контр-ОСИНТ: руководство по приватности

Оглавление

Контр-ОСИНТ: руководство по приватности

Введение

Почему это важно

Базовая цифровая гигиена

Телефонный номер

Почтовый ящик

Фамилия, имя, отчество, дата рождения

Адрес и местоположение

Пароль

Фотография

Утечки баз данных и пробив

Определение источника утечки

Канарейки

Как сделать утечки бесполезными

Приватность телефонных аппаратов

Приватность соцсетей и мессенджеров

Facebook

Telegram

ВКонтакте

Instagram

Приватность для разработчиков

Привязывать телефон к аккаунту - не всегда хорошая идея

Удаление информации о себе

Демонстрация экрана

Россия

Украина

Беларусь

Казахстан

Документы, удостоверяющие личность, в Бразилии: что это и для чего они нужны

Об этом издании

Контр-ОСИНТ: руководство по приватности

Как не дать собрать на себя досье. Руководство для Рунета и стран СНГ.

Издание от 30.10.2026.

Актуальная версия и другие форматы: counter-osint.soxoj.com/pdf

Материалы распространяются на условиях Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0). Вы можете свободно копировать, распространять и перерабатывать их, в том числе в коммерческих целях, при условии указания авторства и распространения производных работ под той же лицензией.

Введение

⊖ Это руководство **не про анонимность**.

Анонимность - это полное скрывание информации о себе, вплоть до личности. Чтобы было невозможно понять, кто вы. Поддерживать анонимность в Сети трудно даже людям из организованных хакерских группировок. Начинать следует с *приватности* - скрывания информации о вашей личной жизни. Поддерживать приватность проще, это как гигиена.

⊖ Это руководство **не про сопротивление большому брату и корпорациям**.

У меня нет цели рассказать вам, как стать неуловимым и не дать заработать на себе большим компаниям. Вы уже в системе, вас уже используют, вы уже товар. А если вы уверенно возражаете и считаете себя анонимным - вероятно, вы находитесь в другой системе, может даже криминальной, и вряд ли почерпнёте здесь что-то новое.

☑ Это руководство **про ценность личной информации**.

Каждый волен сам решать, что ему скрывать. Мне лишь хочется показать, как используются данные, которые вы не скрыли, и как пресечь это использование. Как понять, насколько ценна информация, которую вы собираетесь ввести в окошко и нажать кнопку "Сохранить". Как не продать свои персональные данные по цене шавермы.

☑ Это руководство **про приватность и counter-OSINT**.

Вы узнаете о том, как мыслят люди, которые собирают информацию о вас. Чем они пользуются и руководствуются, какие данные для них важны. Что они с этой информацией могут сделать (и делают!).

И, конечно же, вы получите инструкции по тому, как свести риски потери вашей приватности к нулю. Фактически, это путеводитель для новичков в мир персональной контрразведки.

Добро пожаловать!

Почему это важно

Трудно оставаться вне зоны доступа в наше цифровое время. Отшельник может иметь телефон для экстренной связи, а собака, хоть и не каждая, — аккаунт в Инстаграме.

Проникновение социальных сетей и средств связи могло бы быть исключительно позитивным, если бы не приводило к массе печальных последствий. От звонков фальшивых сотрудников Сбербанка с просьбой продиктовать пароль из СМС, и до коллекторов, внезапно требующих вернуть кредит, взятый на ваш паспорт.

В последние годы появился тренд на приватность и защиту информации о пользователях: GDPR, CCPA, LGBD. Компании обязали заботиться о сохранности персональных данных и о предотвращении их утечек. Но стали они собирать о нас меньше информации? Никак нет. Для них наши данные — источник прибыли.

Но и ужесточения правовых норм для компаний недостаточно. Вы наверняка оставили много “хлебных крошек”, потому что уже не первый год в Интернете. Старые аккаунты, объявления, публичные переписки, фотографии. По этим следам можно вплотную подойти к вам и использовать это в любых целях.

Интересный факт: в 2017 году журналистка нашла анонимные аккаунты директора ФБР всего за пару часов. Достаточно было наводки о его существовании, информации о сыне и о дипломной работе по теологии.

Огромный массив данных о людях, который возможно легко собрать подручными средствами, привёл к популярности OSINT — методологии сбора данных из открытых источников. Часто под этим термином сейчас подразумевают средства слежки за людьми, хотя изначально это методология разведки. Любое средство можно использовать как в благих, так и в плохих целях — об этом следует не забывать.

Поэтому важно иметь средства **Counter-OSINT** — инструменты для защиты своих данных и обеспечения приватности.

Что будет в следующих главах

Разберём простые, но эффективные шаги, которые сильно затруднят сбор информации о вас стороннему наблюдателю. С конкретными пунктами и действиями.

Руководство будет полезно самому широкому кругу заинтересованных — не только тем, кто что-то слышал про OSINT, но и друзьям, знакомым, родителям. Инвестиция в полчаса на вдумчивое чтение и осознанные действия принесёт спокойствие и защиту от мошенничества, слежки, преследования, шантажа.

При этом не будем пренебрегать удобством. Многие руководства концентрируются на том, чтобы обезопасить себя по максимуму (даже если это не оправданно). Мы же будем исходить из необходимости соблюдения **баланса между приватностью и удобством**, при котором пользование Интернетом не будет осложнено.

Напомню, что OSINT — это сбор информации из открытых источников. Но, к сожалению, часто в Сеть попадают такие чувствительные данные как базы номеров телефонов, паспортных данных и так далее.

Мало того — в РФ через “пробив” можно получить подробные сведения о владельце номера телефона, машины, квартиры из официальных государственных реестров и баз данных. К сожалению, многие люди готовы за деньги предоставить доступ к тому, что должно быть тщательно защищено.

Будем считаться с этим: невозможно обеспечить полную анонимность и удалиться из всех реестров, но возможно усложнить процесс поиска настолько, что злоумышленник не сможет зацепиться за информацию.

Таким образом, цель руководства — научить защищать общедоступные сведения и усложнять процесса поиска других сведений про вас.

Определяем важную информацию

Чтобы понять, какие данные важнее и что следует больше защищать, необходимо знать современные реалии с поправкой на Рунет. Это мы и разберём далее, и чтобы попытаться быть объективными, используем OPSEC.

Термин OPSEC, как и OSINT, пришёл из американской разведки. Он означает процесс анализа и защиты критически важной информации.



Болтать - врагу помогать!

Для начала перечислим все **первичные данные**, которые так или иначе раскрывают нашу личность, но *существуют физически вне Интернета*.

- Фамилия, имя, отчество
- Дата рождения
- Паспортные данные (серия, номер и т.д.)
- Физический адрес
- Личные документы (водительское удостоверение и т.д.)
- Биометрические данные
- Прочая личная и идентифицирующая информация

Таких данных не так много. Но, имея хотя бы часть, можно притвориться вами и обмануть третьих лиц. Например, разослать знакомым сообщение с просьбой срочно перевести деньги из-за трудной ситуации.

При этом мошенники не обязательно будут заинтересованы конкретно в вашей личности. Например, они могут купить базу и сотни “свежих” паспортов, чтобы привязывать паспортные данные к электронным кошелькам QIWI для увеличения лимитов по выводу денег.

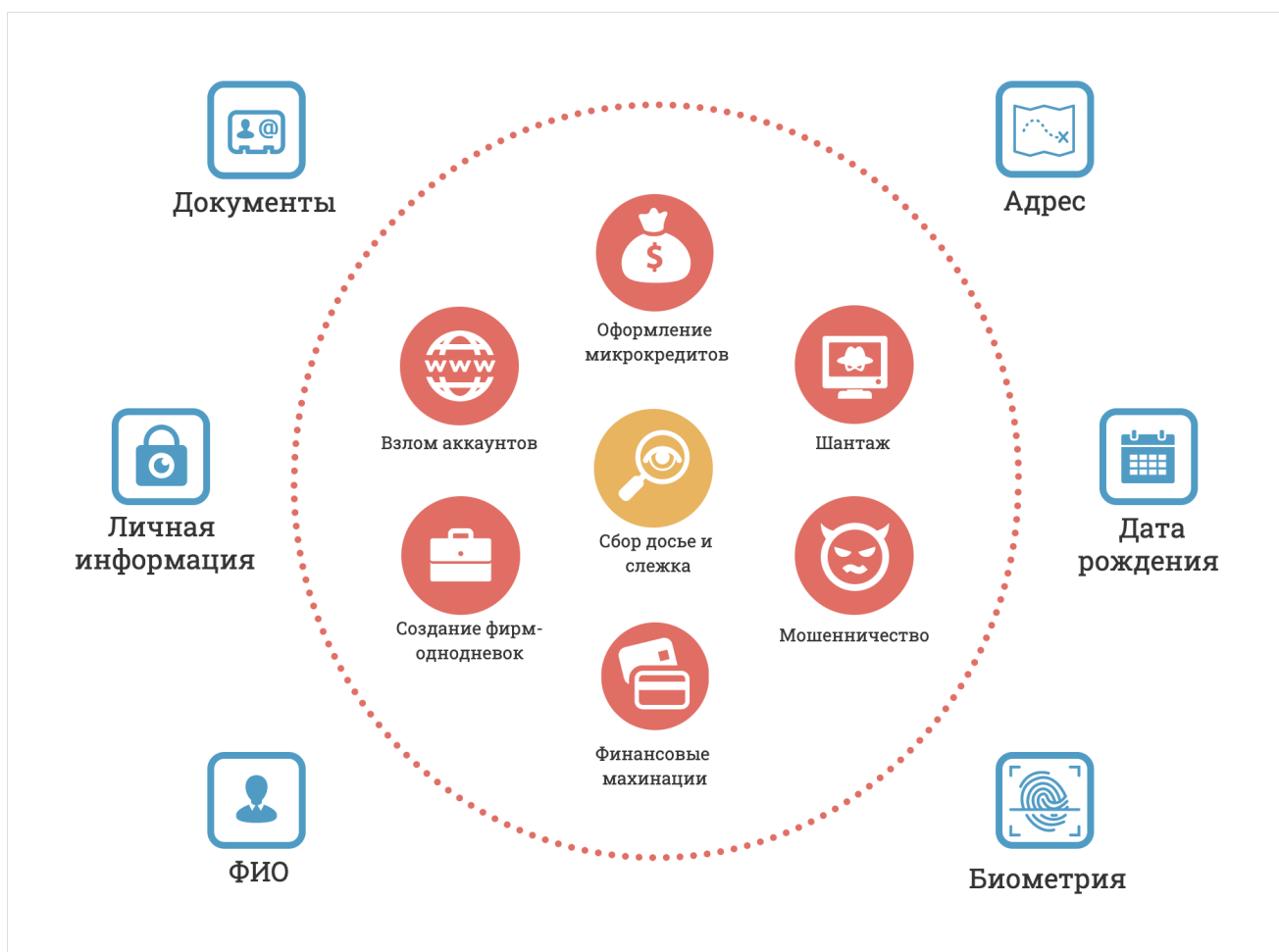
Любые личные данные могут быть использованы. Например, восстановление доступа к аккаунтам социальных сетей часто требует ответить на контрольный вопрос. Таким образом, знание девичьей фамилии матери или любимого музыканта повышает шансы взломать вас.

Интересный факт: в 2012 произошёл громкий случай захвата сразу 4 аккаунтов человека при знании только лишь адреса, имени и email. Элегантная цепочка восстановления доступа — сначала использовать известные данные, потом привязать фальшивые — позволяла сначала завладеть доступом в Amazon, GMail, Apple, Twitter, а потом и вовсе удалённо стереть данные с устройств человека.

Возможно, вас смутил пункт “биометрические данные”, но, увы, их использование уже давно вошло в нашу жизнь. Уже давно распространены средства поиска по лицу, которые используют те же технологии, что и для разблокировки личного телефона через переднюю камеру, а также обширные базы данных из социальных сетей. Когда вы оставляете свою фотографию в Сети, вы оставляете возможность найти себя.

Анализируем угрозы

В соответствии с процессом OPSEC проанализируем, кто может быть заинтересован в подобных действиях и как может использовать информацию о нас. Давайте рассмотрим популярные случаи использования первичных данных на схеме ниже и попробуем сделать выводы.



Что можно сделать с нашими данными?

Что можно сделать с нашими данными? Наверняка вы обратили внимание, что большинство пунктов связано с **получением денег**. Думаю, финансовая мотивация мошенников не требует объяснения. Единственное, что следует отметить — деньги могут быть похищены не только у вас, но и у других лиц. В этом случае критичным для нас становится участие в уголовном процессе, куда могут привлечь как свидетелем, так и обвиняемым.

Выгода от сбора полной информации о вас, включая доступ к перепискам, менее определена. Это может быть как бытовое преследование, так и шпионаж, шантаж и прочее. Ясно только, что в большинстве случаев это **причинение личного вреда и вторжение в частную жизнь**.

Эти угрозы понятны и объяснимы, а во многих случаях регулируются законом. Статьи, связанные с финансовыми потерями, перечислять нет смысла, настолько их много; а сбор личных данных — это 137 УК РФ. Однако, давайте взглянем правде в лицо: требуется серьёзная причина, чтобы идти и самостоятельно форсировать возбуждение дела, а участие

в таких процессах — стресс. Поэтому вернёмся к уже озвученной выше позиции: наша цель в том, чтобы защитить свои данные и избежать угроз.

Очевидно, что знания первичных данных недостаточно для проведения мошеннических схем. Таковые обычно основаны на социальной инженерии и предполагают дистанционное взаимодействие через звонок или сообщения. То есть, мы неявно подразумеваем, что у недоброжелателям уже известны наши **вторичные данные, виртуальные идентификаторы** — номер телефона, электронная почта, адрес аккаунта социальной сети. Таким образом, получение информации об этих данных несет в себе не меньшую угрозу.

Про каждый из типов данных дальше будет рассказано подробнее. А пока оставим своё внимание на том, что чем больше данных попадает в чужие руки, тем серьёзнее может быть исход. Отсюда вывод — количество данных о вас необходимо контролировать, не разбрасывать их где не следует и следить за их использованием.

Поговорим о **цифровой гигиене**.

Базовая цифровая гигиена

Сформулируем нашу цель так: минимизировать количество данных, которые можно собрать о вас в одном месте.

Не класть яйца в одну корзину.

Почему это важно?

Пример 1

Вы пользуетесь услугами компании, которая тратит слишком мало денег на безопасность. В один прекрасный момент их **взламывают**, и вся клиентская база оказывается в руках злоумышленников: телефоны, почтовые адреса, имена, фамилии, ваши покупки. Почти всегда такие базы в итоге оказываются в публичном доступе. В итоге ваши данные станут доступны всем желающим.

Пример 2

Вы пользуетесь услугами компании в высококонкурентном бизнесе, где цена данных клиентов очень высока. Некоторые сотрудники уходят к компаниям-конкурентам, **скопировав** себе клиентскую базу. Каким образом эта база будет использована, и не пойдёт ли она дальше по рукам — нет никаких гарантий.

Пример 3

Вы пользуетесь услугами компании, которая собирает данные своих клиентов, чтобы предлагать скидки и акции. Для этого они рассылают рекламу, пользуясь услугами другой компании. Эта компания делает рассылки постоянно, и заинтересована иметь свои данные по клиентам. Поэтому у второй компании **накапливаются** базы с данными чужих клиентов, которые могут быть потом переиспользованы для других рассылок.

Наверняка у вас возникло возражение: *неужели это никак не контролируется законом? Они не могут легально пользоваться этими данными!*

К сожалению, законодательство в сфере обработки персональных данных (ПДн) не поспевает за реалиями. Обмен виртуальными (не физическими!) данными трудно отследить и пресечь. Более того, рынок

нелегального обмена ПДн настолько развит, что большие игроки лоббируют его легализацию. В таких условиях нельзя положиться на защиту государства или гарантии компаний, и нам необходимо относиться более сознательно к тому, какие данные и в каком количестве мы отдаём другим.

Телефонный номер

Ранее мы говорили, что телефонный номер - это **вторичный** идентификатор. С точки зрения здравого смысла это так: вы можете избавиться от телефона, разорвать контракт с оператором, а может приобрести 100 номеров, и тогда любопытные погрузятся в аналитический паралич, пытаясь с этим разобраться.

Но с точки зрения онлайн-платформ телефон - самое удобное средство связи с вами и подтверждения вашей личности. Поэтому *практически все* используют номер в качестве **первичного**, уникального идентификатора.

Отсюда следует очевидный вывод. Почти любой сайт знает ваш телефонный номер и обладает своими сведениями о вас. Этими сведениями сайт может обмениваться (и делает это!) с другими компаниями - в рамках услуг, за деньги, бартером.

Примеры таких сайтов и платформ: - Системы авторизации в публичном Wi-Fi (97-ФЗ) - Скидочные и дисконтные карты - Авторизация / верификация в социальных сетях и мессенджерах

Соединив все кусочки информации по вашему номеру телефона из разных мест, можно собрать ваш портрет. Что с этим делать?

Разделяем личную жизнь и работу

Почти все мы имеем рабочие и личные дела. Поэтому начать стоит с разделения этих сфер жизни.

Большинство крупных компаний предлагают сотрудникам корпоративную связь: или вы берёте новую сим-карту от компании, или на ваш личный номер подключают рабочий тариф.

Но даже если такой возможности нет, **всегда** заводите отдельный номер телефона. У меня есть несколько аргументов: - Ваши аккаунты невозможно будет связать по номерам автоматически, кроме как через договор с оператором. А это уже высокий уровень защиты! - С отдельным телефоном на порядок легче мыслить в категориях приватности. У вас есть выбор, какой номер привязать к смс-банкингу, а

какой на публичном сайте компании. - Работа есть работа, она должна быть отделена от отдыха и вашей личной жизни. И второй телефон пойдёт только на пользу. :)

Используем виртуальный номер

Можно выделить 3 сегмента сервисов, которые помогают защитить ваш реальный номер телефона.

Сервисы для одноразового приёма СМС

Есть общедоступные сайты, позволяющие принять СМС от любого отправителя. Список их перечислять не будем, потому что их достаточно просто нагуглить по фразе `receive sms online`.

В них используется небольшое количество номеров телефонов одновременно, и часто на них уже заведены аккаунты на разных сайтах: тестировщиками, спамерами, мошенниками. Однако, их можно использовать для авторизации в публичных Wi-Fi сетях. Минус такого подхода только в том, что для получения доступа к публичному интернету вам уже нужен интернет. ☺

Refresh the page every couple of minutes to get new messages.

New messages will arrive every couple of seconds.

Be aware that anyone can see your messages for this number

Please do not verify important information

Update Messages

Give me another number

List of last 50 SMS messages received

From	Body	Date
317043847114	VK: 32796 - use this code to activate your VK profile.	30 minutes ago
317043847114	Demi keamanan akun Anda, mohon TIDAK MEMBERIKAN kode verifikasi kepada siapapun TERMASUK TIM SHOPEE. Kode verifikasi berlaku 15 mnt: 103390	41 minutes ago
33643497658	Greetings from MuslimMatrimony.com Your PIN number is 125967. Use this PIN to verify your Mobile number or give a missed call to 09380054981.	48 minutes ago
31615530128	Uber code: 1790	48 minutes ago
VKcom	Activate, before it not your EDEE DOM IS worth up to 50 euros in exclusive state games. Deal	1 hour ago

- +44 7940406246
- +44 7376493559
- +44 7399305426
- +44 7398668365
- +44 7983238372
- +44 7399533453
- +44 7376494399
- +44 7398668366
- +34 681999929
- +34 681993330
- +972 552992025
- +972 552992024
- +380 999134159

Разумеется, подобные сервисы не рекомендуется использовать для получения чувствительной информации и привязывания к своим личным аккаунтам, так как полученные сообщения и коды доступа может увидеть кто угодно.

И небольшой совет: перед попыткой использования номера с любого из таких сайтов следует обратить внимание на время получения последнего СМС-сообщения (таблица на скриншоте выше). Если это время далеко в прошлом, то номер уже не работает, но его ещё не убрали с сайта.

Сервисы для приёма СМС под конкретный сайт

The screenshot displays the 'SMS Reception' website interface. The top navigation bar includes links for 'Софт', 'Новости', 'Инструкции', 'Контакты', and 'API', along with flags for Russia and the Russian Ruble (XXX Р). A sidebar on the left contains a menu with options like 'Свернуть панель', 'Прием СМС', 'Аренда номера', 'Мобильные прокси', 'История СМС', 'Партнерская программа', 'МОЙ АККАУНТ', 'Оплата', and 'Выписка'. The main content area is titled 'Прием SMS' and features tabs for 'Страны', 'Сервисы', and 'Операции'. The 'Страны' tab is active, showing a list of countries for selection. The 'Сервисы' tab is also visible, showing a list of services and their associated costs.

1. Выберите страну

Россия	Украина
Германия	Британия
Франция	Испания
Швеция	Нидерланды
Дания	Португалия
Канада Virtual	США

2. Выберите сайт или приложение

☆ ВКонтакте	31.5Р
☆ Facebook	15Р
☆ Mail.ru	26.5Р
☆ Viber	9.5Р
☆ Одноклассники	26.5Р
☆ Instagram	11Р
☆ Google (Youtube, Gmail)	12Р
☆ Яндекс	6Р

Сервисы постоянных виртуальных номеров телефонов

Некоторые операторы связи предлагают клиентам **подменный номер** для входящих и исходящих вызовов и SMS бонусом к основному тарифу — без отдельной сим-карты. Подменный номер работает через приложение оператора, и его можно сменить в пару кликов, оставив основной номер прежним.

Так устроено, например, у российского оператора **Т-Мобайл**: подменный номер входит в базовый тариф и меняется из приложения. Похожие возможности есть у Yota, МТС («Второй номер») и ряда зарубежных операторов.

Главное правило: нигде не сохранять подменный номер — ни в адресной книге, ни в профилях. Это позволит регулярно его менять без последствий: как только на него посыпется спам, генерируете новый.

Типовые сценарии использования: - запросы прайсов у компаний с формой «оставьте заявку»; - регистрация на одноразовых ресурсах (акции, розыгрыши, опросники); - доступ к публичным Wi-Fi с SMS-авторизацией.

Для более полной защиты подменный номер имеет смысл комбинировать со скрытым e-mail — связка закрывает большинство бытовых регистраций, в которых ваши основные контакты никому не нужны.

⚠ **Слабое место — человеческий фактор.** Если при регистрациях указывать настоящее имя, цепочку аккаунтов на одном подменном номере всё равно можно связать. При использовании схемы указывайте псевдоним.

Почтовый ящик

Адрес электронный почты был и остаётся самым распространённым идентификатором для аккаунта в Сети. У вас может не быть телефонного номера, но у вас должен быть ящик - это неписанное правило.

Наличие электронной почты само по себе раскрывает о вас некоторую информацию. Прежде всего, это **алиас**, имя ящика, слева от символа собаки “@”. Первый и очевиднейший совет – не стоит выбирать именем ваши инициалы, фамилию и год рождения, если это не сугубо личный или рабочий ящик.

Второй, но немаловажный совет – внимательно изучите провайдера электронной почты. Наиболее известные бесплатные сервисы почты “вдогонку” к email дают вам аккаунты в других продуктах. Это относится прежде всего к Google и Яндекс, так как эти компании ведут свой бизнес в большом количестве других сфер, и предоставить вам бесплатный ящик за то, что вы станете пассивным потребителем десятка других сервисов – их хлеб.

Разделение аккаунтов

Чтобы усложнить поиск информации о вас, рекомендуется использовать ящики с умом: используя техническую возможность создания вариаций ящиков. Согласно официальным соглашениям, после алиаса и перед знаком @ вы можете указывать дополнительный суффикс с “+”, например `nickname+facebook@google.com`. Письма на такой электронный ящик будут приходить к владельцу `nickname@google.com`, но с точки зрения сайтов это будет совершенно другой ящик. У Google, к тому же, существует особенность: любые точки в алиасе рассматриваются как опциональные и работают как суффиксы после “+”.

Существует несколько схем использования: уникальный ящик для каждого сервиса, уникальный ящик для каждой “личности” либо использование только для некоторых сервисов по известной только вам схеме.

Дополнительные преимущества использования суффиксов и точек описаны [здесь](#). Также вы можете проверить использование своего почтового ящика на разных сервисах с помощью инструмента [mailto_analyzer](#).

Долой ящики для подписок, мусора и спама

Отдельно стоит отметить привычку большого количества людей использовать отдельный “мусорный” почтовый ящик для некритичных сервисов и разнообразных спам-подписок. Само по себе разделение почтовых ящиков полезно, но только если оно сознательно (см. выше).

Если же вы не заглядываете в такой ящик, и письма там лежат непрочитанными тысячами и более, то это важный сигнал: разберитесь, действительно ли вам нужен этот ящик. Если нет, то отпишитесь от всех рассылок и удалите связанные с ним аккаунты, чтобы минимизировать вероятность использования этого email-адреса для сбора информации о вас.

Одноразовые ящики электронной почты

Существует большое количество сервисов, предоставляющих одноразовые почтовые ящики на 10-15 минут. Они хороши для одноразовых регистраций на сайтах, куда вы попадаете в первый раз и больше, скорее всего, не воспользуетесь. Здесь рассмотрим те сервисы, которые создаются на случайных доменах.

Сервисы, генерирующие правдоподобно выглядящие алиасы (имя.фамилия):

- [TemporaryMail](#)
- [MinuteInbox](#)

Другие популярные сервисы: - [10minutemail](#) - [TEMPMAIL](#) - [Mohmal](#)

Общедоступные ящики электронной почты

Также в Интернете можно найти сервисы, которые дают возможность использовать **ваш алиас** для временного ящика. Такие почтовые адреса удобно использовать для сервисов, в которых email должен выглядеть правдоподобно.

Примеры таких сервисов:

- [Maildrop](#)
- [Mailsac](#)
- [templail+](#)
- [Yopmail](#) - также поддерживает пересылку (см. ниже)

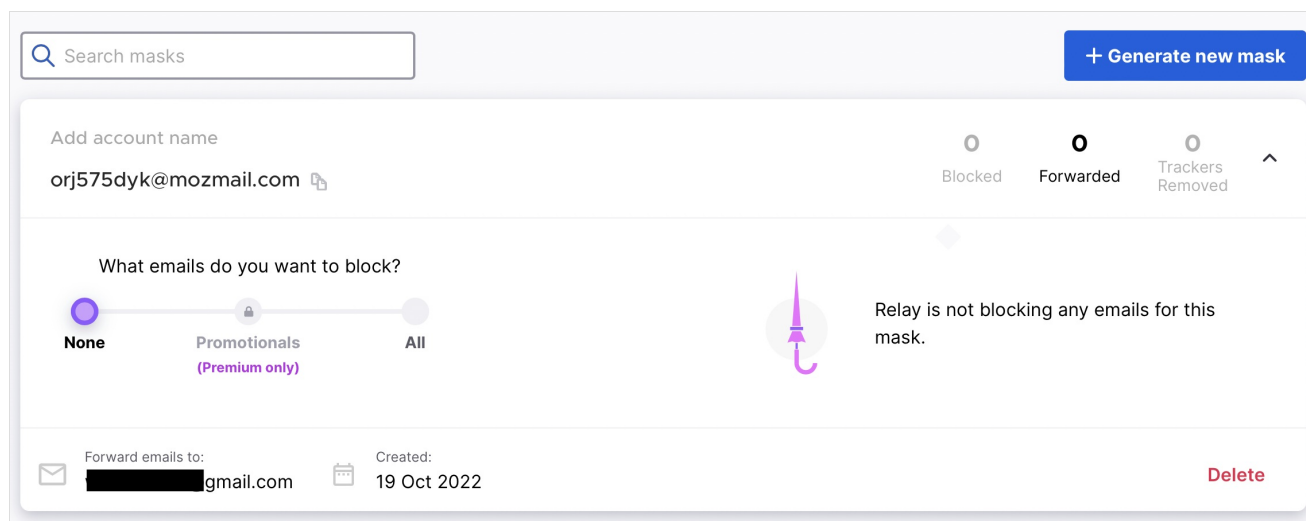
Пересылка почты с других почтовых ящиков

Сервисы, которые позволяют пересылать письма используют, так называемые “маски”, позволяющие скрыть ваш настоящий электронный адрес.

Принцип работы очень простой: - Адрес-маска получает письмо - С этого адреса идет пересылка письма на ваш настоящий адрес

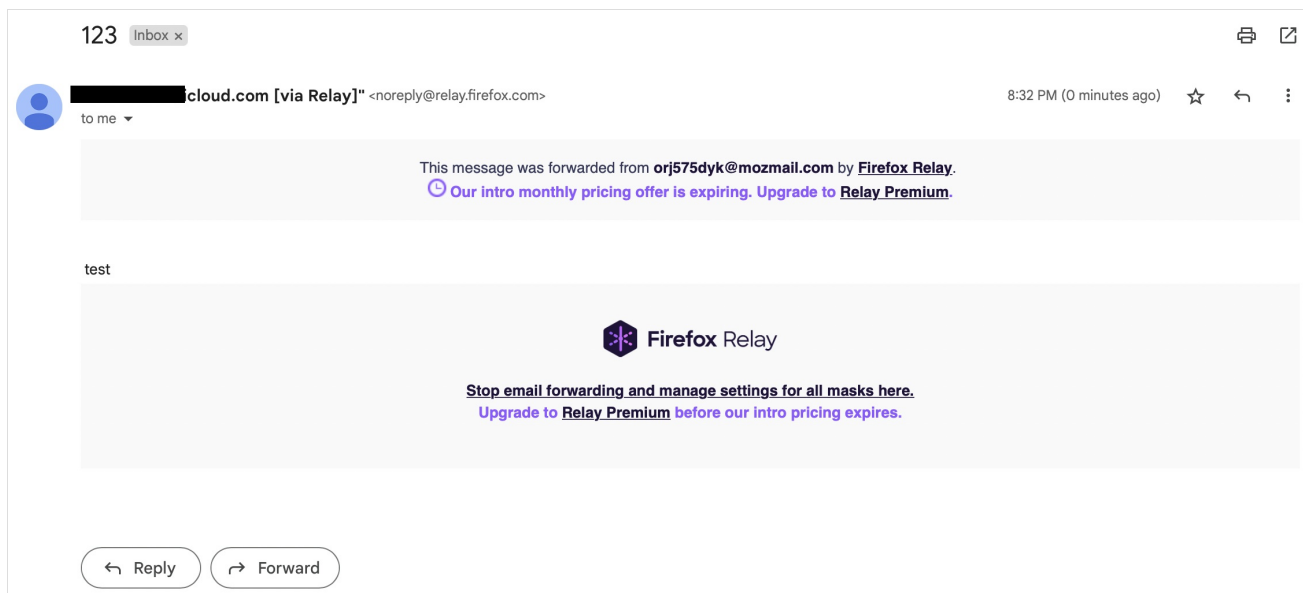
Пример на основе Firefox Relay:

Сначала предоставляется маска, которая скрывает настоящий адрес.



firefoxrelay

Теперь, используя данный адрес-маску мы можем получать письма на свой электронный адрес, не показывая его всему Интернету.



relayedemail

Раздел будет дополняться

Примеры сервисов:

- [SimpleLogin](#)
- [AnonAddy](#) - делает адреса по шаблону `*@ivanov.anonaddy.com`
- [Firefox Relay](#) - делает случайные адреса на домене `mozmail.com`
- [erine.email](#) - делает адреса по шаблону `*.ivanov@erine.email`

Скрыть e-mail (Apple Hide My Email)

Apple даёт пользователям подписки **iCloud+** свой сервис маскирования почты — «Скрыть e-mail». Он доступен из настроек Apple ID на любом устройстве Apple и в браузере на `iCloud.com`, а при регистрации в Safari и в системном приложении «Пароли» предлагается как опция в поле ввода адреса.

Генерируются одноразовые адреса вида:

```
6g662b5nbb@privaterelay.appleid.com
gains-unworn0x@icloud.com
argosy-07raving@icloud.com
```

Письма с них пересылаются на «настоящий» ящик, привязанный к Apple ID; на них можно отвечать, и получатель увидит только маску. Адрес пересылки можно сменить в любой момент, а ненужные маски — удалить: после удаления поток писем и спама на эту маску сразу прекращается.

► Продвинутый уровень

Фамилия, имя, отчество, дата рождения

Почему эта информация вынесена в отдельный раздел? Как правило, ФИО и даты достаточно, чтобы найти конкретного человека, так как вероятность совпадения всех этих данных у двух людей очень низкая.

Государственные учреждения

В различных областях действуют нормы, обязывающие или поощряющие публикацию документов с персональными данными. С одной стороны, открытость в этих областях помогает прозрачности в отрасли (например, госзакупки, списки прошедших/выпускников), но нас более волнует, что, однажды попав в такой документ, нам будет сложно из него удалиться.

К России относятся следующее: - списки абитуриентов в университетах: часто выкладываются с полными ФИО, количеством баллов, из года приказа о зачислении можно сделать вывод о возрасте; - информация об индивидуальных предпринимателях, руководителях и учредителях компаний (ЕГРЮЛ/ЕГРИП); - публичные картотеки судебных дел: однажды совершив правонарушение и даже сумев оправдаться, вас можно будет найти по истории дел; - общедоступные телефонные базы: большей частью содержат неактуальную информацию, но с привязкой к дому и квартире; - публичные реестры задолженностей и залогов; - и так далее.

Раздел будет дополняться

Вход через другой сайт (Single sign-on)

Современная архитектура авторизации и регистрации в онлайн-сервисах предполагает активное использование сторонних “проверенных” учётных записей. Например, почти везде в зарубежном сегменте интернета есть возможность входа через Facebook, в то время как в России всё больше распространяется вход через VK. В каких-то сервисах это подразумевается неявно, например, вход в YouTube через Google-аккаунт.

Если вы таким образом авторизуетесь на неосновном и общедоступном устройстве (например, телевизор или игровая приставка), то есть риск

раскрытия о себе публично отображаемой информации, например, имени и фамилии. Для минимизации этого риска стоит переименовывать аккаунт с “Имя Фамилия” на что-нибудь нейтральное, например, “Аккаунт”.

Адрес и местоположение

Для начала выделим несколько сущностей, на которые имеет смысл обращать внимание с точки зрения OPSEC.

Это: - геолокация: ваше местоположение в реальном времени, которое чаще всего утекает по цифровым каналам; это могут быть как координаты, так и адрес до квартиры; - адрес постоянной регистрации: то, что чаще всего называют “пропиской” - анахронизм постсоветской России, требуемый во многих государственных системах, но почти везде вытесняемый следующим адресом - адрес фактического проживания: адрес, по которому вы “временно зарегистрированы”, также требуемый различными законами и актами для возможности оказания вам различных услуг.

К сожалению, в отличие от США, где ваш адрес = ваш почтовый ящик, в России адрес строго привязан к физической недвижимости. Поэтому у нас невозможны фокусы с “кочевничеством” как в Техасе или Южной Дакоте, где вам необязательно иметь место жительства. Однако, есть возможность использовать абонентские ящики, о чём сказано ниже.

Как предотвратить утечки адресов

- Не публикуйте фотографии в “сыром” виде, файлами. Часто они содержат информацию о месте съёмки.
- Если пользуетесь доставкой, указывайте минимально необходимое количество информации в стандартных полях адреса. Самый предпочтительный вариант - указать лишь номер дома и встретить курьера снаружи. Всё остальное (этаж/квартира/домофон) пишите в поле дополнительной информации — курьер его легко прочтёт, а вот в базу данных с вашим адресом такая неструктурированная информация попадёт с меньшей вероятностью.

Использование абонентских ящиков

В России есть единый государственный оператор почтовой сети: Почта России. Он осуществляет большинство почтовых отправок.

Для доставки обычно используется адрес пребывания человека и его имя, т.е., необходимо указывать ФИО, почтовый индекс, а также полный

адрес, включая номер квартиры. Обычные письма или извещения о заказных письмах/посылках доставляются почтальонами вплоть до почтового ящика на двери дома или в подъезде многоквартирного дома.

Однако, существует возможность анонимной для отправителя доставки писем с использованием абонентских ящиков. Это выделенный ящик для почты в конкретном почтовом подразделении. Каждый ящик имеет свой номер, онлайн можно выбрать любой незанятый, например, 777. Также при договоре заключении аренды ему можно присвоить произвольное имя - это платная (и относительно дорогая) услуга. Единственный минус с точки зрения приватности - для аренды ящика необходимо создать аккаунт на abox.pochta.ru, указав свой номер телефона и паспортные данные.

После заключения договора вы получите ключ от ящика, и можете открыть его в любое время. Но важно понимать, что ящики расположены на территории почтовых отделений, и доступ к ним регламентирован его временем работы. Поэтому удобнее выбирать самые большие отделения, где абонентский отдел работает круглосуточно. В Москве, например, это почта на улице Мясницкой, индекс 101000.

Каким образом теперь отправлять письма? В качестве адреса просите ваших корреспондентов указывать только индекс и номер ящика. Возьмём примеры выше.

Каноничная запись: 101000, а/я 777

Или же коротко: 101000, 777

А если вы присвоили ящику имя “Свалка”, то: 101000, свалка

Правила доставки отправлений касаются и абонентских ящиков. Это значит, что для заказных писем вам будут класть только извещения, и для их получения необходимо продиктовать работнику абонентского отдела номер телефона, получить смс, и только после этого вам выдадут письмо. Но обычные письма, конечно, будут класть прямо в ящик.

Пароль

Главный принцип: **Никогда не используйте одинаковые или похожие пароли**

По двум причинам: - Имея вашу почту и пароль от сайта 1, кто-нибудь обязательно попробует зайти с ними на сайт 2 - и дело не лично в вас, рынок продажи взломанных аккаунтов очень большой, а это товар. - Если данные о ваших аккаунтах вместе с паролями всплыли в утечках, то получится сопоставить между собой даже совершенно разные почты и номера телефонов (хороший пример).

Но как держать в голове много паролей? И где их брать? Советую не относиться ко всем паролям как к данным, которые всегда должны быть у вас в голове. Экономьте место у себя в памяти.

Самый оптимальный способ: создание одного достаточно длинного пароля-фразы для хранилища паролей (или для учётной записи, к которой привязан ваш браузер, в котором хранятся все пароли).

Раздел будет дополняться

Как придумывать стойкие пароли

Стандартные рекомендации по использованию 8 символов, которые включают в себя специальные символы, буквы, цифры не работают! Ведь P@ssw0rd тоже подходит под эти требования, а это не самый крутой пароль, поэтому давайте разбирать методы для создания стойких паролей.

Три случайных слова

Существует простой, но действенный метод для создания паролей - метод 3-х случайных слов.

В чем заключается данный метод? Когда мы регистрируем новый аккаунт, мы просто придумываем 3 случайных слова и ставим их как наш пароль, например: NETWORKINGHYGIENEDEVELOPMENT согласитесь, это намного легче запомнить, чем: asndjBDHJBSDhjSBADHJadbzhjF, да и простым перебором по словарю перебрать такое будет достаточно сложно.

Такие пароли можно усилить, используя LEET, заменяя *некоторые* буквы на цифры, то есть наш пароль будет иметь следующий вид: `N3TW0RKHY6I3N3D3V3L0PM3NT` Таким образом наш пароль становится более стойким, при этом его сложность для запоминания увеличивается не на много, а если вы были знакомы с LEET, до этого, то вам будет еще проще.

Для еще большей стойкости можно разделять слова при помощи разных спецсимволов, например: `- , ~ , =`.

Русские слова в английской раскладке

Еще один простой, но действенный метод - использование случайных русских слов в английской раскладке.

Мы просто берем случайные слова на русском языке и пишем их в английской раскладке, например из `ехалгрекачерезреку` мы можем получить следующее `t[fkuhtrfxthtphtre`.

Выглядит интересно и довольно стойко, но можно дополнять символами/цифрами в конце, например: `t[fkuhtrfxthtphtre123!`
`t[fkuhtrfxthtphtre34345!`

Раздел будет дополняться

Менеджеры паролей

Это то, чем должен пользоваться каждый! Вспоминаем главный принцип из первой строки и сразу в голову приходит вопрос - “Ну, мне что теперь, запоминать 100 паролей!?!?”. Нет, не нужно запоминать 100 паролей, требуется один, это пароль от менеджера паролей.

Менеджер паролей позволит генерировать стойкие пароли и хранить их в одном, а что главное - безопасном месте.

Обзор популярных менеджеров паролей можно прочитать в данной статье - [Обзор менеджеров паролей](#)

Личной рекомендацией составителей руководства будет сервис Bitwarden. Для личного использования его хватит с головой, бесплатная версия включает хранение неограниченного количества паролей, использование с неограниченного количества устройств и все основные функции менеджеров паролей. Помимо хранения паролей, также можно

хранить свои номера банковских карточек и заметки. Генератор паролей позволяет сгенерировать стойкий пароль и проверить его в утечках, что несомненно является одной из “Killer Feature”.

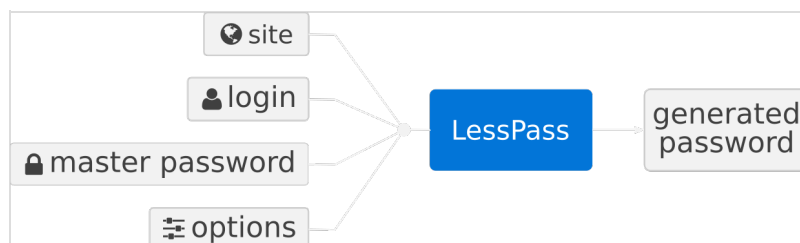
LessPass

Что если вам сложно хранить пароли и синхронизировать их между разными устройствами? На помощь приходят парольные менеджеры без необходимости что-то хранить!

LessPass - не единственная подобная программа, но одна из известнейших. Её концепция в том, что генерация одноразовых паролей происходит на лету при помощи функции, результат которой всегда одинаков при условии одинаковых параметров.

Программе надо сообщить: - мастер-пароль - логин на сайте - адрес сайта

После этого она без какой-либо отправки данных или сохранения чего-либо куда либо сгенерирует ваш пароль. В любой момент на любом устройстве вы можете запустить эту программу — и получить свой пароль для конкретного сайта.



The image shows the LessPass web application interface. At the top, there is a dark header with the 'LessPass' logo and three icons: an information icon, a settings gear, and a share icon. Below the header, the form is organized into several sections. The first section contains a domain input field with 'yandex.ru' and a user input field with 'test@yandex.ru'. The second section is a password field, currently masked with dots, which is highlighted with a blue border. To the right of the password field are three icons: a key, a cube, and a bird. The third section, titled 'Опции' (Options), contains four checked checkboxes: 'a-z', 'A-Z', '0-9', and '%!@'. The fourth section has two controls: 'Длина' (Length) set to 16 and 'Счётчик' (Counter) set to 1, each with minus and plus buttons for adjustment. At the bottom is a large blue button labeled 'Создать и скопировать' (Create and copy).

Полезные материалы и ссылки на источники

- Свободный менеджер паролей LessPass работает на чистой функции

Фотография

К сожалению, фотографии (и вообще любые изображения) уже давно стали легко распознаваемым и индексируемым контентом. Поисковики могут искать похожие фотографии, различать на них текст, предметы, конкретных людей. Социальные сети могут распознать вас на произвольной фотографии и поставить там отметку со ссылкой на вас даже без вашего ведома.

Но, к счастью, в последние годы тренд на приватность усилился, и поэтому соцсети вводят разумные ограничения на распознавание людей. Универсальные поисковики от точного поиска по лицам тоже отказываются: Google не ищет людей по лицу принципиально, а Яндекс ищет похожие изображения и на практике нередко находит человека, но отдельной функции «найти по лицу» у него нет. Это снижает вероятность злостного использования таких функций, но не мешает использовать подобные технологии в целом. Сейчас инструменты распознавания можно легко создать самостоятельно либо использовать условно-бесплатные аналоги.

Раздел будет дополняться

Как проверить себя

На постсоветском пространстве для поиска по фотографии лица всё ещё можно использовать Яндекс. Но одного его мало: ниже — сервисы, которые ищут именно лица, а не похожие картинки.

Если вы активно использовали социальные сети, то можете обнаружить не только свой аккаунт, но и фотографии с вашим лицом в аккаунтах ваших друзей, знакомых или других людей, которые даже не имеют к вам отношения. Разумеется, такие фото удалить чрезвычайно затруднительно, и если вы не хотите, чтобы они указывали на вас, то следует грамотно удалить аккаунт.

Фотографии профиля Вконтакте

Всего лиц в базе: 1,109,563,766 (просчитано 100% от всех).
Время сбора: с 11-2019 по 11-2020. Используется улучшенный алгоритм распознавания. Процент успешных поисков: 68.79%.

[Перейти](#)

Аватарки Вконтакте и Одноклассников

Всего лиц в базе: 280,781,743 (просчитано 67% ok.ru и 100% vk.com).
Время сбора: vk.com: с 12-2018 по 06-2019, ok.ru: с 06-2019 по 03-2020. Процент успешных поисков: vk.com: 46.90%, ok.ru: 45.19%.

[Перейти](#)

Аватарки Тиктока

Всего лиц в базе: 125,443,334 (просчитано 18.38% от всех).
Время сбора: с 03-2021 по 09-2021. Процент успешных поисков: 10.52%.

[Перейти](#)

Аватарки Одноклассников (Новая база 2022 и алгоритм)

Всего лиц в базе: 126,280,848 (просчитано 77% от всех).
Время сбора: с 01-2022 по 02-2022. Процент успешных поисков: ??.%.

[Перейти](#)

Аватарки Клубхауса

Всего лиц в базе: 13,071,041 (просчитано ~65% от всех).
Время сбора: с 05-2021 по 01-2022. Процент успешных поисков: ??.%.

[Перейти](#)

Публичные персоны

Всего лиц в базе: 55,741,249. Время сбора: с 05-2022 по 08-2022. Процент успешных поисков: ??.%.

[Перейти](#)

Специализированные поисковики по лицам

Нишу, от которой отказались универсальные поисковики, заняли отдельные сервисы. Ограничений на поиск людей у них нет по определению — в этом весь их смысл. Проверять себя стоит каждым из них: индексы у них разные, и пустой результат в одном ничего не говорит про остальные.

- Search4Faces — **бесплатный, регистрация не нужна** (платный у него только API). Ищет по аватаркам и фотографиям профилей ВКонтакте, Одноклассников, TikTok и Clubhouse — то есть смотрит ровно туда, куда PimEyes и FaceCheck.ID не заглядывают. Базы у него устаревшие, большая часть собрана в 2022 году и раньше, и это работает в обе стороны: там до сих пор лежит аватарка, которую вы сменили сто лет назад, но и пустой результат сегодня не значит, что вас там нет. База неполная, и на незнакомое лицо сервис нередко выдаёт просто похожих людей.
- VK.watch — архив ВКонтакте: профили, их правки, друзья, фотографии и комментарии, включая те, что вы давно удалили. Поиск по лицу там тоже есть, отдельной кнопкой. Этим сервис и неприятен: удаление фотографии во ВКонтакте не убирает её из

архива, снятого раньше. Доступ по платной подписке, а среди подписчиков, по их же FAQ, адвокаты, рекрутеры и частные детективы.

- Geometria — поиск по фотоархиву репортажей: клубы, вечеринки, городские мероприятия. Загружаете селфи и находите себя на чужих снимках с событий, куда вы просто пришли и о съёмке не думали. Распознавание платное.
- PimEyes — индексирует открытый веб: новостные сайты, блоги, фотобанки, форумы. Бесплатный поиск покажет, что совпадения есть, но превью будут заблюрены; картинки без блюра и ссылки на страницы-источники доступны по подписке.
- FaceCheck.ID — позиционируется как проверка «не мошенник ли это перед вами», индексирует соцсети, фотографии из полицейских баз, публичные реестры. Счётчик проиндексированных лиц сервис показывает прямо на главной: на момент написания это больше 1,4 миллиарда.

Два последних находят вас там, куда Яндекс и российские архивы не добираются: в чужих фотоотчётах, на сайте конференции, в галерее спортивной секции, на групповом фото с работы.

И общее для всех: проверяя себя, вы загружаете своё лицо в поисковик по лицам. Это осмысленный обмен — узнать, что о вас уже известно, — но всё-таки обмен.

Как убрать себя из поисковиков по лицам

Условия очень разные: от бесплатного удаления по селфи за минуту до письма анонимному владельцу на gmail. А у одного сервиса такой возможности нет вовсе.

FaceCheck.ID. Удаление бесплатное и, по заявлению сервиса, мгновенное: нужно найти себя поиском по собственному фото, отметить свои снимки на странице Remove My Photos и подтвердить личность селфи прямо в браузере.

PimEyes. Форма отказа требует загрузить несколько фотографий лица с разных ракурсов и скан паспорта или удостоверения личности. То есть чтобы вас перестали находить по лицу, нужно отдать сервису

дополнительные фотографии вашего лица и документ. Скан просят обезличить, закрыв всё лишнее, но решать, стоит ли такой размен, всё равно вам.

Geometria. Здесь путь законный, но бумажный: оператор — российское юрлицо, ООО «ГЕОПРОМЕДИЯ», и отозвать согласие на обработку данных можно, отправив скан письменного заявления на law@geo.pro или оригинал заказным письмом. Отзыв удаляет учётную запись и записи с вашими персональными данными, но не сами фотографии: они остаются в репортажах, а контент администрация по соглашению удаляет исключительно по своему усмотрению.

Search4Faces. Формы нет, но есть почта: сервис прямо пишет, что запросить удаление своих изображений из поисковой выдачи можно письмом на search4faces@gmail.com, и обещает ответить в течение суток. Гарантий, кроме этого обещания, никаких — кто владеет сервисом, неизвестно: домен зарегистрирован через багамского регистратора приватности, а переписка идёт с обычного ящика на gmail.

VK.watch. Политика приватности у сервиса есть, и в ней даже описано право потребовать удаления данных письмом на support@vk.watch. Но читать её стоит внимательно: она описывает данные подписчика — почту, платёжные реквизиты, технические логи, историю запросов. Архивных профилей ВКонтакте в перечне собираемых данных нет вовсе, и обязательства убрать вас из архива в ней тоже нет. Право на удаление здесь есть у того, кто ищет, а не у того, кого находят.

Но профилактика надёжнее любого письма: в архиве останется тот снимок, который был сделан при сборе, и сменить аватарку задним числом бесполезно — в этом и смысл архива.

Главное: удаление из индекса не удаляет саму фотографию. Она остаётся там, где лежала — в чужом альбоме, на сайте мероприятия, в новостной заметке — и её переиндексирует следующий сервис. Устойчиво работает только удаление первоисточника: удалить свой аккаунт или попросить владельца сайта убрать снимок.

И эти сервисы — не все, а лишь те, что видны снаружи. Например, Clearview AI собирает такой же индекс, но продаёт доступ только государственным заказчикам, и проверить себя в нём нельзя никак.

Есть и другие закрытые сервисы, которые ищут по индексу фотографий из социальных сетей и даже из мессенджеров, популярных в отдельных странах, — WhatsApp, Telegram и прочих. А там фотография профиля по умолчанию открыта: её видит любой, кто наткнулся на ваш аккаунт в общей группе или нашёл вас по номеру телефона, так что заккрыть её настройками приватности стоит не только от знакомых.

Фото лица как биометрия

Раздел будет дополняться

Клоакинг

Для борьбы с инструментами распознавания людей на изображениях используется так называемый клоакинг. Суть метода в искажении фотографии таки образом, чтобы визуально мы воспринимали её как оригинал, но программы не видели там человека или лица.

Методы для искажения бывают как ручными (блюр/ретушь/искажение отдельных частей фото), так и автоматическими. Из последних можно отметить специальные программы, которые используют алгоритмы распознавания лиц в обратную сторону, модифицируя фотографию так, чтобы поиск был не возможен. Пример такой программы: Fawkes.

Разумеется, подобная постобработка фото или видео не поможет превентивно. Для затруднения распознавания лиц “умными камерами” в реальной жизни придумываются оригинальные и не очень способы, примеры можно прочесть по ссылкам в конце страницы.

Метаданные фотографий

Раздел будет дополняться

Используемые материалы и полезные ссылки

- Большой брат (пока) подслеповат
- Новый макияж короля

Утечки баз данных и пробив

Началось всё ещё в девяностых: на территории бывшего СССР понемногу утекали государственные базы — паспортные, адресные, регистрационные, базы операторов связи. Потом к ним добавилось огромное количество утечек обычных сайтов: магазинов, доставок, форумов, сервисов доставки еды. А в какой-то момент в Рунете расцвели услуги поиска сразу по всему этому массиву.

Под пробивом в этом руководстве имеется в виду именно это — **процедура поиска человека по множеству баз, сайтов и реестров одновременно**. Не единичный взлом, а сложившаяся индустрия, которая по одному вашему телефону или имени собирает всё, что когда-либо куда-либо утекло или где-то публично лежит.

Сделайте это сегодня

Четыре действия, на которые хватит вечера. Подробности и объяснения — дальше в главе, но начать можно прямо с них.

1. **Поищите себя** по номеру телефона и по почте в сервисах проверки утечек. Вы узнаете, в каких именно базах уже лежите, — а дальше станет понятно, что чинить в первую очередь.
2. **Смените пароли там, где они повторяются**. В российских утечках пароль почти всегда лежит рядом с логином, так что один раскрытый пароль открывает все ваши аккаунты сразу.
3. **Включите вход по коду** — двухфакторную аутентификацию — везде, где она есть. Тогда одного украденного пароля уже не хватит.
4. **Заведите отдельную почту** для магазинов, доставок и разовых регистраций. Такие базы утекают чаще всего, и пусть утекает адрес, который не связан с вашими главными аккаунтами.

Дальше — почему это работает именно так и что делать, если данные уже утекли.

Проверьте, что утекло именно про вас

Начинать стоит не с чтения, а с проверки: по телефону, почте или ФИО можно посмотреть, в каких известных утечках вы уже есть. Сервисы для этого и риски каждого разобраны в разделе Поиск себя в утечках.

Главное оттуда: за любым онлайн-поиском может стоять желание дополнить ваш профиль — записать ваш адрес в сети, связать несколько ваших запросов между собой и понять, кого вы ищете. Поэтому надёжнее искать себя в самих файлах утечек, а не через чужой сайт, хоть это и труднее.

Удалить свои данные из утечек нельзя

Никак. Это главный неприятный факт главы, и обойти его нечем.

Попросить популярные сервисы убрать вашу запись из поиска можно, и это стоит сделать. Но сама база от этого не исчезает: к моменту, когда утечка стала публичной, её успели скачать десятки людей, она разошлась по частным сервисам и закрытым ботам, и отозвать все копии невозможно. Запрос на удаление убирает вас из одного окна, а не из данных.

Теоретическая возможность удалиться всё-таки есть, и знать о ней стоит — хотя бы чтобы понимать, кому она доступна. Люди с высоким статусом или служащие в силовых структурах добиваются удаления себя из выдачи давлением на сами сервисы, которые этой выдачей торгуют. Но удаляют так только тех, на кого есть чем надавить, — и у этого есть обидный побочный эффект: **само удаление работает как маркер**. Если человек находится в одном сервисе и отсутствует в другом, из этого видно и то, какие сервисы чистят выдачу, и то, что за конкретным человеком кто-то приходил. А удалиться полностью всё равно не выходит: баз слишком много, и договориться со всеми разом не получится ни у кого.

Это не повод ничего не делать — это повод делать другое.

Что работает вместо удаления

- **Понять, откуда утекло.** Зная, какой сервис вас сдал, вы перестанете давать ему новые данные и заодно увидите, какие ваши зацепки уже связаны между собой. Как это выяснить — Определение источника утечки.

- **Узнать о следующей утечке раньше остальных.** Для этого есть канарейки — подставной адрес или особая ссылка, которые дают вам знать в тот момент, когда кто-то начинает вас искать. Как их расставить — [Канарейки](#).
- **Обесценить то, что уже утекло.** Если к вашему имени в базах привязаны десять правдоподобных, но чужих или выдуманных контактов, цена такой записи падает. Приёмы — [Усложнение использования утечек](#).
- **Убрать себя из сервисов, которые торгуют этими базами.** У многих есть процедура удаления: где-то форма, где-то заявление с паспортными данными, где-то платная подписка. Инструкции по конкретным сервисам и ботам — [Удаление информации об утечках](#).

Что обычно утекает

Утекают не только логины и пароли. Чтобы было видно, насколько это шире, — разберём одну реальную базу по полям, а потом посмотрим на остальные.



image

Это лишь часть одной базы — а таких по всем регионам России собраны сотни.

Как выглядит одна строка утечки

Абстрактно «утекли персональные данные» звучит нестрашно. Поэтому вот реальный состав полей одной базы — медицинской лаборатории «Гемотест», выложенной 1 мая 2022 года:

имя · пол · дата рождения · место рождения · гражданство
паспорт · кем выдан паспорт
свидетельство о рождении · кем выдано свидетельство
СНИЛС / ИНН
номер полиса · страховая компания
адрес · телефон · почта
связь с родственником · номер клиента
дата создания записи · дата обновления записи

Остановитесь на секунду и посмотрите, что это за набор. Человек сдавал анализы — а в одной строке оказались **паспорт, свидетельство о рождении, СНИЛС**, полис, гражданство, место рождения, адрес и телефон. Этого достаточно, чтобы представиться вами в разговоре с банком или оператором связи: такие данные как раз и спрашивают, когда проверяют, что это действительно вы.

Два поля в этом списке стоят отдельного внимания.

Связь с родственником. Ваша утечка автоматически становится утечкой про вашего ребёнка или родителя, даже если сами они в эту лабораторию не обращались.

Даты создания и обновления записи. По ним видно не только что о вас знают, но и когда вы обращались, то есть восстанавливается хронология вашей жизни.

И главное: это лаборатория. Не банк, не госорган, не соцсеть — место, куда приходят один раз сдать кровь.

Известные большие утечки

Несколько российских баз, которые лежат в открытом доступе. В последней колонке — поля, по которым видно, что именно о человеке оказалось снаружи.

Когда утекло	Откуда	Записей	Что в полях
июль 2021	Delivery Club	1,8 млн	почта, имя, телефон, адрес, сетевой адрес компьютера и точные координаты дома
2022	СДЭК, две разные копии базы	66,9 млн и 104,6 млн	почта, имя, телефон, адрес, номер квартиры, имя, зарегистрированное в налоговой , время создания записи
февраль 2022	Яндекс.Еда	~7 млн	имена, телефоны, полный адрес доставки, комментарии к заказу
май 2022	Гемотест	31 млн	паспортный набор (см. разбор полей выше) и результаты медицинских анализов
2023	Росреестр	3,0 млн	имя, адрес, телефон, ИНН, паспорт
январь 2025	Росреестр	25,1 млн	то же плюс почта, дата рождения, СНИЛС и связь с компанией
июль 2025	ЕМИАС, медицинские карты Москвы	около 17 ТБ	данные пациентов и внутренние базы

Для сравнения: в январской утечке Росреестра 25 миллионов записей. На 2024 год в России жило около 146 миллионов человек, в Москве — около 13 миллионов. То есть одна эта база по размеру вдвое больше, чем всё население Москвы.

Три поля отсюда стоит рассмотреть отдельно, потому что они меняют представление о том, что вообще считается «персональными данными».

Точные координаты у доставки еды. Это не текстовый адрес, который можно написать неточно, а точка на карте с точностью до подъезда. Плюс в той же строке сетевой адрес вашего компьютера — то есть и где вы живёте, и откуда выходили в сеть.

Номер квартиры и имя из налоговой у курьерской службы.

Служба доставки хранила не просто адрес, а квартиру, и отдельно — ваше имя в том виде, в каком оно записано у налоговой. Это уже не контакт для курьера, это опознание личности.

Связь с компанией у Росреестра. Человек, его паспорт, его недвижимость и его фирма в одной строке. Для того, кто собирает досье, это самая дорогая связка: она соединяет личную жизнь с деловой.

Сколько утекло всего — не знает никто

Это стоит сказать прямо, потому что цифру «сколько» вы встретите в новостях много раз и каждый раз разную.

Расходятся даже числа по **одной конкретной утечке**. Росреестр, январь 2025: взломщики заявили о двух миллиардах строк, в новостях писали про опубликованный кусок на 82 миллиона, а в сервисах поиска эта база лежит на 25 миллионов записей. Разброс в восемьдесят раз — при том что речь об одном событии. У СДЭК похожая история: в новостях фигурировали 19 и 25 миллионов, а в открытом доступе лежат две разные копии на 67 и 105 миллионов, причём помеченные как «две версии предполагаемой утечки» — то есть спорен даже сам факт.

Годовые итоги расходятся так же. За один и тот же 2025 год государственный надзорный орган насчитал чуть более 52 миллионов утёкших записей, независимые исследователи — от 145 до 767 миллионов, а профильное министерство заявило, что утечек стало в 13 раз меньше, чем годом раньше. Разброс между крайними оценками — более чем в десять раз, и дело не в чьей-то недобросовестности: считают по-разному, а главное — **не все утечки становятся известными**.

Практический вывод из этого один, и он неприятный: отсутствие новости про утечку в сервисе, которым вы пользуетесь, ничего не говорит о том, утекли ли ваши данные.

Чем это отличается по странам

Здесь полезно развести две разные вещи: сколько данных утекло и как к ним получают доступ.

Россия на мировом фоне

Сразу предупреждение: **разные измерения дают противоположный ответ на вопрос «где больше».**

По одному подсчёту Россия на первом месте в мире по числу утёкших аккаунтов на человека. По другому — впереди США, и заметно: около 14,6 миллиарда записей против 4,3 миллиарда у России. Франция, которая в первом рейтинге идёт самой первой, во втором оказывается почти в шесть раз ниже России.

Противоречие объясняется не чьей-то ошибкой, а тем, **что именно считают.** В такие подсчёты попадают очень разные вещи: настоящие взломы, собранные вручную списки паролей, результаты автоматического сбора открытых анкет, базы для рассылок и выгрузки публичных реестров. По опасности они несравнимы, а в общий счётчик идут одинаково. Плюс сказывается внимание тех, кто эти собрания пополняет: англоязычные базы собирают активнее.

Отсюда вывод, который важнее любого места в рейтинге: **«в какой стране больше утечек» — плохо поставленный вопрос.** Ответ меняется вместе со способом подсчёта. Для вас значение имеет не рейтинг страны, а то, какие конкретно базы с вашими данными лежат в открытом доступе, — а это проверяется поиском по себе, а не чтением статистики.

Что видно устойчиво — структура, и она у соседей разная. У России и Украины сверху финансы и торговля, но у Украины на втором месте **государственные базы**, а в первой пятёрке есть автомобильные. У Казахстана первое место делят **государственные базы и образование.** У Беларуси собрано меньше всего, и состоит оно целиком из взломов.

Разрыв между Россией и соседями огромен, но читать его как «в Беларуси безопаснее в тысячу раз» не стоит: маленькое собрание может означать и то, что страной меньше занимались те, кто эти базы складывает.

И отдельная цифра, которая полезнее общего рейтинга: **в российских утечках на 100 украденных аккаунтов приходится 89 украденных паролей**. То есть пароль почти всегда лежит рядом с логином — поэтому повторное использование пароля здесь обходится дороже, чем в среднем по миру.

Откуда в этих сервисах данные

У массива, по которому ищут, два источника.

Государственные и корпоративные базы. Те самые, что утекали с девяностых, и те, к которым доступ продают сейчас — через человека с легальными правами: сотрудника оператора, банка, ведомства. Большинство сделок здесь — не технические атаки, а предательство: паспортные данные и сведения из полицейских баз уходят **от десяти долларов за запрос**.

Показательно, чем закончилась попытка это прикрыть: объявленная в России кампания против рынка пробива ударила в том числе по самим силовикам, которые в нём торговали, а продавцы переехали за границу и продолжили работать оттуда. Доступность данных после кампании не упала.

Утечки обычных сайтов. Их больше по объёму, и именно они дают сервисам пробива связки «телефон — почта — ник — адрес доставки». Одна база интернет-магазина сама по себе безобидна; десять таких баз, сведённых по общему телефону, дают маршрут вашей жизни за десять лет.

На кого Россия похожа по устройству рынка — на Индию. Там то же самое: не взлом, а платный доступ через посредника с законными правами. В одном разобранном случае компания, официально имевшая право проверять личность граждан, выдала наружу ключ доступа, которым посторонние два года проверяли чужие документы по шесть центов за запрос — и никто этого не замечал.

При этом по объёму утечек Индия Россию не догоняет и близко — 562 миллиона записей против 4,3 миллиарда. То есть **объём утечек и устройство рынка доступа — независимые вещи**: страна может утекать меньше, но торговать доступом так же. Защищаться приходится от обоих по отдельности.

Что это значит практически

Если вы в России или другой стране с развитым рынком пробива, то защита «не отдавать данные» работает слабее: основные базы — государственные и банковские, и отдать данные туда вы обязаны по закону. Остаётся второе: следить, какие зацепки — телефон, почта, ник, адрес — связаны между собой, и не давать склеить их в одно досье.

Что именно продаётся в каждой стране и какие документы работают как ключ к вашему досье, разобрано отдельно:

- [Россия](#)
 - [Украина](#)
 - [Беларусь](#)
 - [Казахстан](#)
-

Разобраться, что именно про вас лежит в открытом доступе, и решить, что с этим делать в вашем случае, можно вместе со специалистом — напишите на counter-osint+book@soxoj.com.

Это не поможет удалить данные из утечек: как сказано выше, удалить их нельзя. Но понять, какие именно связки работают против вас и что имеет смысл закрывать в первую очередь, — можно.

Определение источника утечки

Поиск себя в утечках

Существует много сайтов, которые позволяют по телефону, почте или даже ФИО самостоятельно найти себя в утечках информации и слитых базах. Использовать их надо с осторожностью, потому что за любым онлайн-поиском может стоять дополнительная цель в обогащении данных. Например, **сбор IP-адреса**, связывание нескольких поисков одного человека для **сбора информации о его окружении**.

Поэтому предпочтительным вариантом всегда остаётся *самостоятельный поиск в файлах утечек*. Но это может быть затруднительно: надо найти файл (или много файлов, если нужен исчерпывающий поиск), понять его структуру, выполнить эффективный поиск.

Если же вы пошли более простым путём, то рекомендую использовать такие ресурсы, по убыванию рисков:

Общеизвестные безопасные площадки

Самая известная: Have I Been Pwned, поддерживаемая известным безопасником и дающая гарантии приватности.

Другие: - <https://monitor.mozilla.org/>

Коммерческие альтернативы

Часто дают условно-бесплатный доступ, найти разные сайты можно по ключевым словам check, leak:

- <https://leakcheck.io/>
- <https://checkleaked.cc/>

Боты в Telegram

~- https://t.me/PhoneLeaks_bot - поиск источников утечки~- больше не работает

Большинство ботов не указывают источник, из которого получена информация. Список некоторых ресурсов: Google Spreadsheet.

Уведомления

Некоторые из перечисленных выше сайтов также предоставляют функциональность уведомлений вам на почту, если произошла новая утечка с вашими данными. Если вы ведёте активную виртуальную жизнь, то крайне рекомендую пользоваться таким сервисом.

Использование алиасов/фейковых почтовых адресов

Gmail и другие крупные почтовые сервисы поддерживают специальные символы для создания алиасов вашего почтового ящика. Почта, отправленная на алиас, придёт к вам, но в поле “Получатель” вы будете явно видеть, куда она пришла.

То есть, `soxoj@protonmail.com` будет эквивалентен `soxoj+gitlab@protonmail.com`:

From	 GitLab <gitlab@mg.gitlab.com>
To	soxoj+gitlab@protonmail.com

Строго рекомендуется использовать эту возможность во всех сайтах, где она поддерживается. Таким образом: 1. Вы в случае утечек или рассылки спама будете точно знать, откуда была получена почта. 2. В случае целенаправленного сбора информации по вашему email информация с нескольких сайтов с меньшей вероятностью будет объединена в одно досье.

Разумеется, при сборе утечек часто используется нормализация почт: удаление подобных частей алиасов и очистка лишнего. Поэтому можно говорить только про снижение риска, а не стопроцентную защиту.

Отдельно стоит упомянуть про указание почтовых адресов **для отправки чеков** при покупках в Интернете.

Согласно п. 2 ст.1.2 закона № 54-ФЗ, кассовый чек должен быть направлен в электронной форме, если покупатель сообщил свой абонентский номер или адрес электронной почты до момента расчета.

Этим пользуются такие крупные Telegram-боты как Глаз Бога, сохраняя себе всю вашу платёжную информацию и **добавляя указанный email** к той информации, которую выдаёт бот.

Поэтому, если вы не заинтересованы в чеке, то указывайте заведомо неправильный почтовый адрес, указывающий на источник утечки,

например, eyeofgod@recept.com. Либо используйте упомянутые выше алиасы, явным образом раскрывающие, где ящик был указан.

Использование разных имён для отслеживания

Кроме непосредственно поиска себя в базах, вы можете проактивно оставить “маячки”, по которым быстро найдёте сайт или компанию-виновника. Чаще всего в жизни это происходит при спам-звонках, в которых упоминают ваше имя, например, указанное на сайте с объявлениями.

Сайты по-разному относятся к корректности имени и фамилии аккаунтов. Кто-то требует того, чтобы они совпадали с паспортными данными (например, в ВК), кто-то только сверяет их с документами в случае финансовых операций, а большинство вообще не валидируют.

В зависимости от строгости правил сервиса (ToS, Terms of Service) можно использовать трюки, перечисленные ниже. Но перед использованием я настоятельно советую изучить, какие санкции возможны, если вы укажете некорректное имя, и оценить эти риски для себя.

Используем имена/фамилии, созвучные либо начинающиеся с тех же букв, что и сайт/компания.

Таким образом, при утечке ФИО в связке с номером или почтой вы будете знать, откуда эта информация:

- Макдональдс: *Максим*
- ВКонтакте: *Вова*
- Одноклассники: *Олег*

Используем вариации имени кириллицей или латиницей

Прежде всего это относится к полной/сокращённой форме имени:

- Александр
- Саша
- Саня
- Шура

Но в силу различий между языками, у имени бывает по несколько “латинских” форм. Даже банки часто дают возможность выбора правильной транслитерации имён. Так, имя “Анатолий” может быть представлено как:

- Anatoly
 - Anatolii
 - Anatoliy
-

► Продвинутый уровень

Пройти это по своим данным вместе со специалистом — определить источник утечки, завести подставные адреса и имена для разных сервисов и потом увидеть, какой из них сдал вас первым, — можно по адресу counter-osint+book@soxoj.com.

Канарейки

Канарейки очень чувствительны к примесям опасных газов в воздухе. Поэтому долгое время шахтёры брали их с собой в шахты: если птица переставала петь, то это значило, что дышать воздухом становится опасно.

Подобный же принцип используется и в информационной сфере. Многие компании используют уведомление пользователей о том, что за ними никто не следит, чтобы при получении судебного ордера *убрать* эту фразу. Тем самым компания даёт сигнал пользователям, что отсутствие слежки больше не гарантируется.

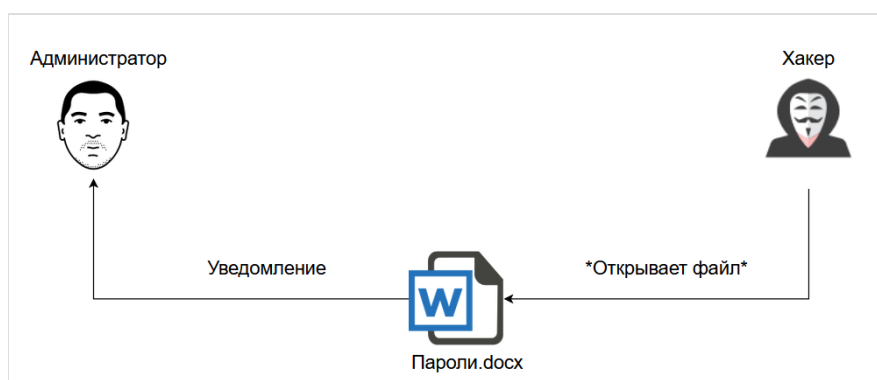
Но мы собираемся скрываться не от корпораций, а от любопытных лиц. Что мы можем предпринять?

Canary tokens

Возможно, вы видели ссылки в биографии на странице ВК, которые никуда не ведут (либо ведут в приложение “Узнай, кто за тобой шпионит” или вроде того). Это простейшая форма канарейки.

Существует замечательный онлайн-сервис - Canary Tokens, который позволяет создавать своих собственных канареек.

Он позволяет создать различного рода канарейки, которые мы можем использовать для детектирования любопытных сотрудников вашей организации или обнаружить компрометацию ваших систем еще до того как злоумышленник сможет выполнить некоторые деструктивные действия.



Какие виды можно сгенерировать и при каких условиях будет получено уведомление: - URL-токен. При переходе по ссылке. - DNS-токен. При разрешении доменного имени. - AWS-ключи. При использовании ключа AWS. - Microsoft Word/Excel Document. При открытии файла. - Kubeconfinfing. При использовании Kubeconfig. - WireGuard VPN. При использовании конфига. - Cloned Website. При клонировании веб-сайта. - MySQL Dump. При загрузке дампа MySQL. - Windows Folder. При попытке открыть папку. - Fast Redirect. При попытке посетить сайт, с последующим перенаправлением. - Slow Redirect. При попытке посетить сайт, с последующим медленным перенаправлением, для получения большей информации. - Custom Image Web Bug. При просмотре вашей картинки. - Acrobat Reader PDF Document. При открытии PDF документа в Adobe Reader. - Custom exe / binary. При запуске исполняемых файлов. - SQL Server. При загрузке базы данных SQL Server. - SVN. При открытии папки SVN. - Unique email address. При отправке почты на электронный адрес.

Пример уведомления на почту:

Canarytoken triggered

ALERT

A DNS Canarytoken has been triggered by the Source IP 213. [redacted] Please note that the source IP refers to a DNS server, rather than the host that triggered the token.

Basic Details:

Channel	DNS
Time	2022-05-31 17:43:23 (UTC)
Canarytoken	yao4fmvql0okrz4oi5tla70yq
Token Reminder	pwned
Token Type	windows_dir
Source IP	213. [redacted]

Canarytoken Management Details:

Manage this Canarytoken [here](#)

More info on this token [here](#)

Powered by: [Thinkst Canary](#)

[Canary](#)

Раздел будет дополняться

Отличие от фишинга и ссылок-логгеров

Раздел будет дополняться

Как сделать утечки бесполезными

Можно ли сделать утечки менее полезными при сборе информации о вас? Да, хоть это и не гарантированно поможет, а лишь усложнит жизнь тем, кто собирает про вас данные.

Разберём некоторые стратегии сопротивления, подходящие для случаев, когда данные о вас уже попали в Интернет.

Создание нового фейкового аккаунта

Создаём аккаунт с идентификаторами, которые используются в активном поиске по данным из утечек.

Раздел будет дополняться

Фальшивые связи с общеиспользуемыми идентификаторами

Почты:

```
a@mail.ru
test@example.com
mail@mail.ru
l@ya.ru
work@mail.ru
work@bk.ru
work@list.ru
1234@mail.ru
test@test.ru
```

Номера телефонов:

```
+79123456789
+79111111111
```

Сайты для генерации правдоподобных данных

- <https://randomuser.me/>
- <https://www.fakenamegenerator.com/>
- <https://www.behindthename.com/random/>

Раздел будет дополняться

Приватность телефонных аппаратов

Тема приватности на мобильных устройствах заслуживает отдельного большого путеводителя. Данные пользователя представляют слишком большой финансовый интерес для всех вендоров. И если на западном рынке наблюдаются подвижки в сторону приватности (например, Apple урезает возможность сбора данных всем сторонним приложениям, а Google с каждой версией Android улучшает работу с доступами приложений), то на азиатском рынке (Samsung, Xiaomi и масса мелких вендоров) пользовательские данные оседают в больших количествах и бесконтрольно.

Что с этим можно сделать за короткое время и без сложных манипуляций вроде получения root или jailbreak? К сожалению, самый минимум - следить за тем, какие приложения вы ставите и какие разрешения им даёте. Разберём самые очевидные случаи.

Контакты из телефонной книги

Многие приложения сделали свой бизнес только лишь на доступе к телефонной книге пользователя. Самое нашумевшее - GetContact, которое пришлось волной и по российским пользователям. Принцип прост – связка из имени контакта и телефонного номера из вашей книги утекают на сервера, там объединяются в одну базу данных. После чего становится возможным узнать ФИО по номеру телефона, запросив напрямую в базе. А иногда и профессию, и возраст, и вообще что угодно. Для примера: “Иван ФСБ”, “Александр Клиент”, “Валерия Хрущёва 42”, “Машка Петрова Якобы Модель”. Сейчас все эти данные можно легко получить через Telegram-ботов.

Некоторые другие приложения (например, вполне официальные вроде Сбербанка) запрашивают доступ к телефонной книге, чтобы сократить телодвижения для переводов по номеру телефона на пару кликов. При этом, очевидно, контакты в любом случае загрузятся к ним на сервер, и что там с ними произойдёт - неизвестно.

Поэтому первым и очевидным шагом в сторону приватности (как себя, так и своих близких и знакомых) будет ограничение доступа к телефонной книге – не даём его приложениям по запросу, т.к. они

должны функционировать без него (Сбербанк прекрасно обходится и без этого). В противном случае внимательно изучаем приложение и ищем альтернативы, если оно безоговорочно требует дать ваши номера.

Устанавливаемые приложения

Продолжая тему из предыдущего абзаца: приложения для сбора контактов работали не только явно, но скрыто, внедряясь за деньги в другие, бесплатные приложения. Таким образом, большое количество невнимательных людей сами сливали свои данные, не обращая внимание на то, что очередная игра из Google Play запрашивает слишком много расширений. А лицензионные соглашения в наше время мало кто читает, увы.

Используемые материалы и полезные ссылки

- [Список сервисов и приложений-альтернатив, нацеленных на приватность](#)
-

►  Продвинутый уровень

Приватность соцсетей и мессенджеров

В этом разделе приведены описания настроек приватности для всех популярных сайтов и платформ на территории СНГ.

Напоминаю, что это руководство направлено на **скрытие** вашей информации от чужих глаз в Сети. К сожалению, практически всё, что вы пишете в соцсетях и мессенджерах, доступно самим платформам. То есть, большому количеству сотрудников этой компании, правоохранительным и другим органам, имеющим право эту информацию запрашивать, а также иногда большому количеству других лиц, полулегально поддерживающих деятельность сайта.

Полностью защититься от утечки своей личной информации - не пользоваться никакими платформами, не гарантирующими end-to-end шифрование и абсолютную безопасность ваших данных, но таких сайтов чрезвычайно мало, и их распространённость среди ваших друзей и знакомых наверняка близка у нулю.

В текущий момент оставим в стороне размышления о том, использовать или нет большие сайты, зарабатывающие на вас деньги и готовые продать ваши данные. Примем как факт, что вам приходится их использовать, и займёмся их настройкой.

Раздел будет дополняться

Facebook

Обсудим настройки приватности в самой популярной соцсети по всему миру - в Facebook. Как и в других главах, убираем общедоступность и по возможности ставим максимальные уровни, комментируя их предназначение и сопутствующие риски.

Для начала разберём уровни приватности, которые Facebook позволяет выставить для своей информации и публикаций.

- **Доступно всем / Все** - информацию будут видеть как все пользователи Facebook, так и весь Интернет - доступ будет открыт поисковикам.
- **Друзья** - информацию будут видеть только ваши друзья.
- **Только я** - информация будет отображаться только вам.
Максимальная приватность!
- **Настройки пользователя** - гибкий настраиваемый список тех, кто может и кто не может видеть информацию. Доступны как отдельные люди, так и категории “Друзья” и “Друзья друзей”.

Также для “Друзей и подписок” есть дополнительные уровни видимости “Друзья, кроме...” и “Определённые друзья”, которые являются вариантами последнего.

Важное замечание: уровень “Друзья” предполагает, что этой группе людей вы можете доверять больше, но не стоит недооценивать возможности социальной инженерии. Вы можете без долгих раздумий подтвердить запрос на добавление в друзья человека, похожего на вашего знакомого. Который на деле таковым не окажется, а добавится исключительно ради получения вашей приватной информации.

Заходим в раздел “Настройки и конфиденциальность” => “Быстрые настройки конфиденциальности”. Открываем первую карточку “Кто может видеть ваши публикации” и последовательно разбираем экраны с настройками.

Кто может видеть ваши публикации

Информация профиля

- *Электронный адрес и Дата рождения* - на деле эти данные нас идентифицируют, ставим *Только я*.
- *Родной город и Город проживания* - если они различаются, то третьи лица могут легко связать информацию о вас в молодости/до переезда с текущей информацией. В таком случае также рекомендуется ставить *Только я*.
- *Образование* - аналогично предыдущему пункту (эта информация может выдавать ваш родной).
- *Работа* - обычно не представляет тайны, если это публичная работа. Зависит от вашей ситуации.
- *Кто может видеть список друзей в вашем профиле? и Кто может видеть людей, Страницы и списки, на которые вы подписаны?* - информация о социальном графе потенциально даёт возможность узнать про вас многое из вышеперечисленного косвенным образом. Наверняка у вас в друзьях есть и сослуживцы, и одноклассники, и одноклассники. Поэтому также ставим “Только я”.

Публикации и истории

- *Будущие публикации* - определяет, какое значение будет выставлено по умолчанию для новых постов. Позволяет избежать случайной публикации поста с неверными настройками приватности. Рекомендуется выставить “Друзья”.
- *Истории* - они видны только 24 часа, но не только в Facebook, но и в Messenger. Не пренебрегаем рисками узнать информацию о нас через ещё одну платформу, поэтому выставляем “Друзья”.
- *Ограничить доступ к старым публикациям* - **важная настройка**, которая даёт возможность массово сменить настройки видимости для всех старых публикаций. Нажимаем “Ограничить доступ” и подтверждаем своё решение.

Блокировка

В этом разделе можно добавлять людей в чёрный список. Нашей целью сейчас это не является, но если вы озаботились приватностью, зная о конкретном подозрительном профиле - заблокируйте его здесь.

Как люди могут находить вас на Facebook

Этот раздел в “Быстрых настройках конфиденциальности” **очень важен для нас** - он позволяет “разорвать связь” между вашим телефоном и почтой и аккаунтом.

Запросы на добавление в друзья

Как уже упоминалось выше, добавление может быть инициировано только лишь ради того, чтобы увидеть ваши приватные данные.

Номер телефона и электронный адрес

Обе настройки выставлены во “Все”. Это означает, что номеру телефона и адресу электронной почты вас можно найти через встроенный поиск Facebook! Разумеется, ставим “Только я”.

Поисковые системы

Эта настройка включена по умолчанию и разрешает индексацию вашего профиля. Выключаем и тем самым запрещаем находить наш профиль в результатах поиска по имени Google, Yandex и т.д.

Используемые материалы и полезные ссылки

- [Хабр - Настройки приватности Facebook VS OSINT](#)

Telegram

Перейдём к настройкам приватности в мессенджере, который считается одним из самых приватных - в Telegram. Как и в других главах, убираем общедоступность и по возможности ставим максимальные уровни, комментируя их предназначение и сопутствующие риски.

Заходим в настройки, раздел “Конфиденциальность”. Начнём с одноимённого подраздела.

Конфиденциальность

Telegram даёт возможность гибко управлять белыми и чёрными списками по доступу к вашим данным. Для пунктов в этом подразделе можно скрыть информацию от всех или показать всем либо использовать список ваших контактов. Также возможно добавлять точечно исключения в виде отдельных аккаунтов или всех людей, состоящих в определённых группах.

Контактами в данный момент в Telegram считаются не только те аккаунты, для которых вам известен телефон (так было ранее), но и аккаунты, вручную добавленные в контакты приложения. Поэтому полагаться на список контактов в настройках сильно не следует – как минимум, в вашей телефонной книге уже могут быть посторонние номера, а контакты внутри приложения легко добавить по ошибке. Поэтому рекомендуется сделать ревизию телефонной книги либо вообще не расшаривать к ней доступ. Подробнее смотрите в разделе доступов для мобильных приложений.

Номер телефона

Ставим опцию “Кто видит мой номер телефона” в значение “Никто”, иначе любой аккаунт в Telegram в любом чате сможет видеть ваш номер телефона.

Также видим, что есть опция “Кто может найти меня по номеру”. Это одна из наиболее ценных настроек приватности Telegram. Она была добавлена исключительно из-за массовых протестов в Гонконге и недовольства протестующих из-за той лёгкости, с которой полиция могла раскрывать их номера.

К сожалению, до сих пор эта опция не имеет значения “Никто”. Ставим эту опцию в “Мои контакты”, и теперь только аккаунты из ваших контактов смогут добавить вас по номеру телефона. Помним при этом ограниченное доверие к группе контактов (см. выше).

Последняя активность

В платформе есть особенность – ограничения на время последней активности (был N минут назад в сети) действует в две стороны. Ставим в значение “Никто”, но помним, что при этом и вы не сможете видеть активность других аккаунтов. К счастью, конкретных людей при необходимости можно добавить в исключения и удалить после проверки.

Группы и каналы

Разрешение на добавление вас в группы и каналы имеет ограничение – нельзя запретить всем, но можно разрешить только своим контактам. Также для опции действуют отдельные точечные запреты.

Ставим опцию в значение “Мои контакты”. Помним при этом ограниченное доверие к группе контактов (см. выше).

Звонки

Антиспам в Telegram работает хорошо, поэтому звонки от спамеров довольно редки. Также, к счастью, сам звонок не раскрывает о вас никакой информации, если не включён режим Peer-to-peer. В этом режиме Telegram устанавливает прямое соединение от вашего устройства к устройству собеседника, и становится возможным определить IP-адрес.

Ставим “Кто может мне звонить” в значение “Мои контакты”, если вы готовы добавлять вручную аккаунты в контакты и следить за их “чистотой”. Ставим опцию “Peer To Peer” в значение “Никто”.

Фотография профиля

При включённой опции другие аккаунты теряют возможность видеть ваш аватар. Эта довольно полезная опция тоже ограничена уровнем доступа контактов, но также может быть включена вручную для конкретных аккаунтов.

Ставим опцию в значение “Мои контакты”. Помним при этом ограниченное доверие к группе контактов (см. выше).

Пересылка сообщений

С определённой версии Telegram научился для пересланных (forward) сообщений убирать ссылку на автора. Таким образом, даже если ваше сообщение скопируют в другой чат, через него невозможно будет выйти на ваш профиль. Ранее это позволяло отслеживать аккаунты, которые оставили хотя бы одно сообщение в любом чате.

Ставим опцию “Кто может ссылаться на мой аккаунт при пересылке сообщений” в значение “Никто”.

Раздел будет дополняться

Настройки

Общее

Блок “Настройки профиля”. Включаем опцию “Скрывать блок подарков”.

Приватность

Для **всех настроек** в списках ниже сначала выставляем “Только я”, при необходимости добавляем людей через опции “Только друзья”, “Некоторые друзья” или “Все друзья, кроме...”.

Моя страница

- Кто видит основную информацию моей страницы
- Кто видит мои сохранённые фотографии
- Кто видит список моих групп
- Кто видит список моих аудиозаписей
- Кто видит список моих подарков
- Кто видит моих скрытых друзей

В блоке “Кого видно в списке моих друзей и подписок” выбираем всех друзей и все подписки.

Записи на странице

- Кто видит чужие записи на моей странице
- Кто может оставлять записи на моей странице
- Кто видит комментарии к записям
- Кто может комментировать мои записи

Фотографии

- Кто может отмечать меня на фотографиях
- Кто видит фотографии, на которых меня отметили
- Кто видит местоположение моих фотографий

Заходим в панель управления “Отметки на фото” и снимаем все галочки: - Распознавать меня на фото. Алгоритмы ВКонтакте будут предлагать вам фотографии , на которых вы сможете отметить себя - Показывать друзьям распознанные фото со мной. Друзья увидят в ленте фотографии с вами и смогут отметить вас. Подтвердить отметку можете только вы. - Распознавать друзей на моих фото. Алгоритмы будут предлагать вам отметить друзей на ваших фотографиях - Показывать блок «Это вы на фотографии?» в ленте. В ленте появится блок, где вы сможете подтвердить или удалить отметку - Показывать блок «Это друг на фото?» в ленте. Искусственный интеллект найдёт на фотографиях ваших друзей и предложит их отметить

Связь со мной

“С кем устанавливать прямое соединение в звонках” - выбираем “Только друзья”

“Кто может найти мой профиль при импорте контактов” - выбираем “Никто”

“Что видно вместо моего фото при импорте контактов” - выбираем “Картинку с буквой”

Истории

- Кто может видеть мои истории
- Кто может отвечать историями на мои истории
- Кто может отправлять мнения к моим историям
- Кто может видеть поздравления для меня в историях

Прочее

“Кому в интернете видна моя страница” - выбираем “Только пользователям ВКонтакте”

“Какие обновления видят в новостях мои друзья” - снимаем все отметки

“Тип профиля” - “Закрытый”

“Кто видит количество моих шагов в Шагах ВКонтакте” - выбираем “Только я”

“Кто может видеть мою активность в играх” - выбираем “Никто”

“Кто может видеть мою активность в мини-приложениях” - выбираем
“Никто”

Настройки приложений

Раздел будет дополняться

Instagram

Раздел будет дополняться

Приватность для разработчиков

Раскрытие своего почтового ящика

При работе с программным кодом и такими системами контроля версий как git существует риск раскрытия своего персонального почтового ящика. Часто это происходит при одновременной работе с личными/рабочими проектами на одном устройстве.

Чтобы избежать этого, проверяйте корректность глобальных настроек или настроек в директории конкретного репозитория:

```
git config --global user.name  
git config --global user.email
```

GitHub предоставляет возможность скрывать ваш email из интерфейса и блокировать “утечку” основного ящика, привязанного к аккаунту:

☒ **Keep my email addresses private**

We'll remove your public profile email and use `20349640+martinovacc@users.noreply.github.com` when performing web-based Git operations (e.g. edits and merges) and sending email on your behalf. If you want command line Git operations to use your private email you must [set your email in Git](#).

Commits pushed to GitHub using this email will still be associated with your account.

☒ **Block command line pushes that expose my email**

When you push to GitHub, we'll check the most recent commit. If the author email on that commit is a private email on your GitHub account, we will block the push and warn you about exposing your private email.

Настройки приватности почтовых ящиков в GitHub

Раздел будет дополняться

Привязывать телефон к аккаунту - не всегда хорошая идея

Не используйте подтверждение через номер телефона там, где это необязательно.

2FA используется для усиления безопасности. Используйте дополнительный фактор для входа в сайт, когда вы осознаете, что аккаунт на конкретном сайте для вас важен (переписки, покупки, финансы), и что вы сознательно будете подтверждать вход каждый раз.

Однако, если есть выбор, что именно использовать для подтверждения, - номер телефона либо *что-то другое* - то используйте другое. Компании заинтересованы в том, чтобы знать ваш номер: рассылать вам СМС, проверять вашу личность, связывать её с другими сайтами. Так же легко они выдадут часть вашего номера при попытке входа в ваш аккаунт или когда ваш друг даст приложению доступ к своим контактам.

Также плохой идеей будет привязывать чужой телефон. Например, привязать телефон бабушки к своему аккаунту в Google, потому что Google зачем-то потребовал от вас добавить телефон. Зная ваш аккаунт, будет возможно получить часть номера телефона бабушки через, например, восстановление доступа.

Где вообще возможны утечки информации о ваших учётных записях?

- Форма входа. Например, сервис может отвечать сообщениями “пользователь с таким email не существует” и “вы ввели неправильный пароль”, что однозначно подтверждает наличие аккаунта с вашим почтовым ящиком.
- Форма регистрации. Сайт не даст вам зарегистрировать аккаунт на телефон, который уже есть в системе: “этот телефон уже используется”. А если его там нет, то на телефон скорей всего отправится уведомление.
- Форма восстановления доступа. Чаще всего вводятся одни данные, например, никнейм аккаунта, а сервис отвечает что-то вроде **Новый пароль отослан на ящик iva*****ov@mail.com** или **Мы отослали СМС на номер,**

оканчивающийся на 93 . Или просит ввести email, а потом пишет “если такой аккаунт существует, то мы отправили уведомление”. А Meta (Facebook) достаточно знать только ID аккаунта.

Во всех этих местах возможна утечка второго фактора (номера телефона), который вы привязываете к аккаунту.

Удаление информации о себе

Удаление собственных аккаунтов

Прежде чем удалять — найдите, что удалять. По одному нику обычно находится больше аккаунтов, чем вы помните сами: старые форумы, сервисы, куда регистрировались один раз, площадки с автоматической регистрацией через почту. Для быстрой самопроверки подойдёт бот Maigret — он ищет аккаунты по имени пользователя на тысячах сайтов, устанавливая ничего не нужно.

Несмотря на то, что интернет всё помнит, удаление аккаунтов остаётся одним из самых сильных средств против базовой разведки по вам. Кажется, что это тривиальная тема, но есть несколько важных нюансов:

Перед удалением: 1. Запросите у сервиса **выгрузку своих личных данных** по GDPR. Это поможет на следующих шагах и даст вам понимание того, что сервис знает о вас. 2. **Переименуйте свой аккаунт**, удалите/поменяйте фото, выждите несколько дней. Это необходимо, чтобы сайты-индексаторы и поисковики успели обновить информацию про ваш аккаунт, и впоследствии вас нельзя было найти по его последней копии. Также не забывайте, что с этого момента нельзя оставлять какие-либо комментарии и сообщения публично. 3. Все старые комментарии/твиты/сообщения **желательно удалить**. В соцсетях и мессенджерах есть механизмы, позволяющие выйти на вас даже после удаления: упоминания (ссылка на ваш профиль, выглядящая как имя), пометка авторства, репосты/ретвиты. От всех подобных зацепок стоит избавиться. 4. Обновите выдачу поисковиков, попросив их переиндексировать вашу **изменённую страницу** (Google) и подождите некоторое время, чтобы другие системы, сохраняющие информацию из соцсетей, также получили новую версию вашего аккаунта.

После этого аккаунт можно удалять встроенными средствами платформы.

Запрос на удаление

Не во всех сервисах удаление возможно штатными средствами. Или же оно спрятано так глубоко, что найти его невозможно. К счастью, есть вспомогательные сайты с информацией о том, как удалиться.

- [JustDeleteMe](#) - прекрасный каталог по платформам, даёт ссылки и описание нужных действий, показывает сложность удаления. Также у создателей есть родственные сайты [JustGetMyData](#) и [JustWhatsTheData](#) для выполнения пункта 1 выше.
- [AccountKiller](#) - инструкции по удалению для большого количества сайтов, преимущественно западных.

Даже если вы не смогли найти инструкцию по удалению для нужного вам сайта - не отчаивайтесь. Всегда остаётся возможность написать в поддержку и запросить удаление вашей учётной записи согласно GDPR.

Удаление выдачи в поисковиках

Google предлагает целый ряд различных форм, через которых можно запросить удаление и обновление контента в поисковой выдаче.

- [Удаление устаревшего контента из поиска](#) - хорошо подходит для страниц, которые нужно переиндексировать (см. выше п. 4 про удаление аккаунтов).
- [Форма запроса на удаление личных данных в Google](#)
- [Новая форма запроса на удаление личных данных](#)

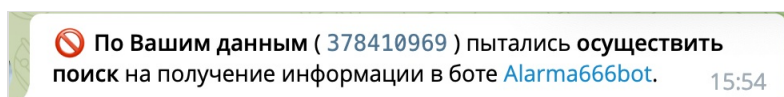
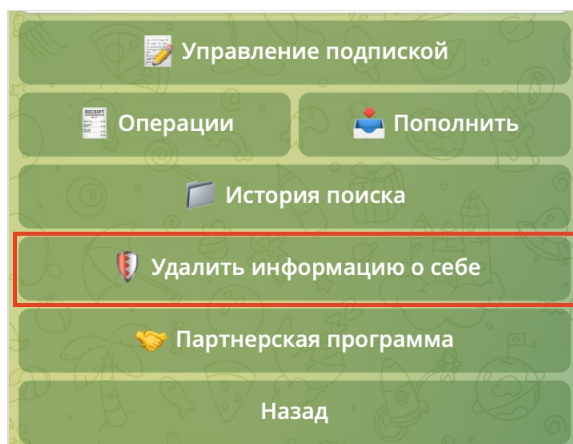
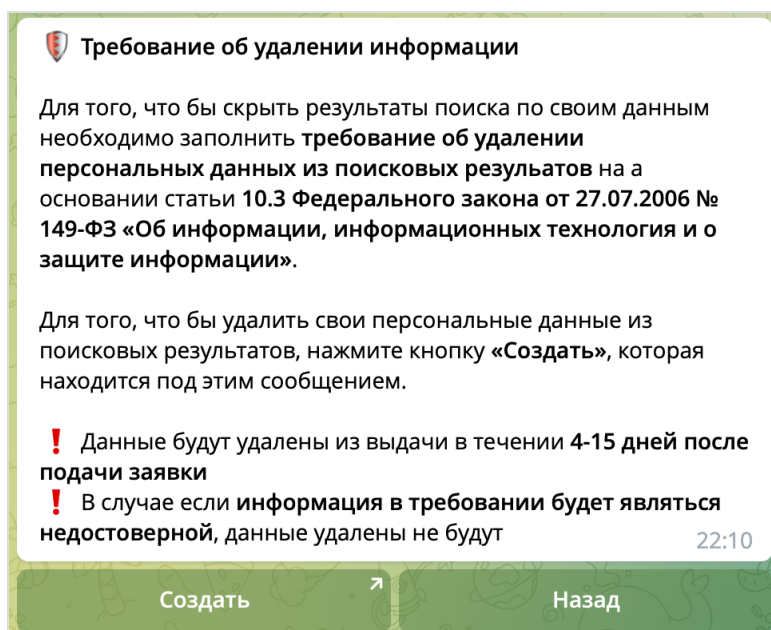
Удаление информации об утечках

[Краткие инструкции по удалению ваших данных из популярных сервисов](#) - Have I Been Pwned, Leakcheck, IntelX и т.д.

Для заявок в сервисы, которые заинтересованы в хранении ваших данных, необходимо готовить полный перечень всей информации, которую вы хотите подчистить. Он должна включать: - никнеймы - телефоны - почты - адреса - госномера автомобилей - государственные идентификаторы (номер паспорта, СНИЛС, ИНН, ФИО и т.д.) - любые данные из строк слитых баз данных

Удаления себя из Telegram-бота Глаз Бога

В Глазе Бога реализован запрос на удаление личных данных в пункте меню Аккаунт бота. После заполнения анкеты с ФИО, номером телефона, датой рождения и e-mail заявка рассматривается несколько дней. После принятия заявки введенные вами данные удаляются из поиска другими людьми, а при попытке поиска вы получаете уведомление.



Требование об удалении персональных данных из поисковых результатов Глаз Бога.

Для того, что бы удалить свои персональные данные из поисковых результатов, заполните форму анкеты требования, которая находится на данной странице. Пункты, помеченные «*» – являются обязательными.

Анкета требования

Заполните данные формы.

ИНФОРМАЦИЯ О ЗАЯВИТЕЛЕ:

ФИО *

Дата рождения *

mm / dd / yyyy

Телефон *



Электронная почта *

ДОПОЛНИТЕЛЬНЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, КОТОРЫЕ ПОДЛЕЖАТ УДАЛЕНИЮ:

Введите персональные данные из поисковых результатов (если таковые есть) в нужные формы ниже.

Г/Н автомобиля

Адрес

ИНН

СНИЛС

Требование на удаления персональных данных из поисковых результатов Глаз Бога.

Здесь отображаются Ваши запросы на удаления данных



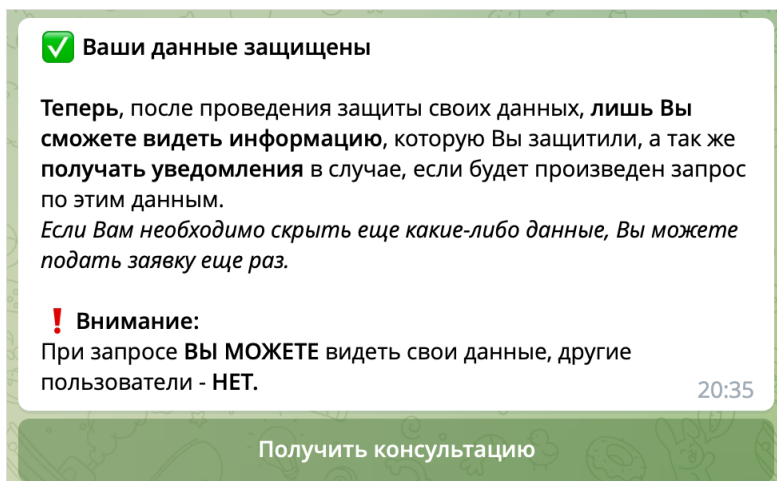
Запрос №123456789

Иванов Иван Иванович

На проверке

9 сек. назад

В случае удовлетворения требования, ваши персональные данные указанные в требовании будут удалены из поисковых результатов в течение 10 (десяти) дней.



Блокировка поиска по себе из Telegram-бота TELESINT

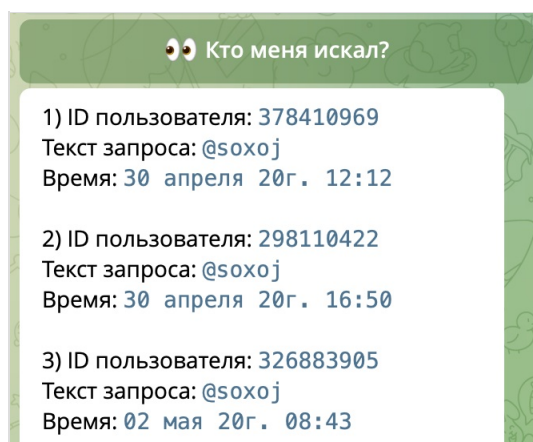
TeleSINT предоставляет возможность скрывать себя от поиска, присылать оповещения, если вас пытаются найти через бота, а также просматривать список тех, кто вас искал. К сожалению, для этого **нужна платная подписка**.

Платный доступ в себя включает:

- 1 месяц — 500 рублей (~6.8\$, ~206€)
- 3 месяца — 1000 рублей (~13.5\$, ~415€)
- 6 месяцев — 2000 рублей (~27.1\$, ~824€)

Список услуг, входящих в платную подписку:

- Полный безлимит на количество запросов в сутки!
- Вы будете скрыты от поиска (режим невидимки);
- Оповещение о том, что вас пытаются найти;



Скрытие данных о себе из Telegram-бота Quick OSINT

В Политике обработки персональных данных сервиса сказано:

Срок обработки персональных данных является неограниченным. Пользователь может в любой момент отозвать свое согласие на обработку персональных данных, направив Оператору уведомление @Quick_OSINT_support с пометкой «Отзыв согласия на обработку персональных данных».

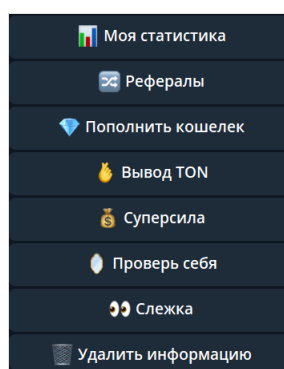
Все запросы на удаление обрабатываются вручную, необходимо заполнить заявление о блокировке данных из общедоступных источников с указанием полных паспортных данных, адреса бота, а также идентификаторов для блокировки, после чего отправить его фото или сканированное изображение Оператору. Данные удалят в течение 7 дней.

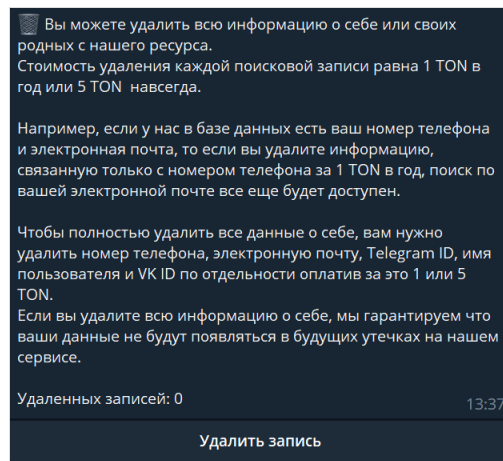
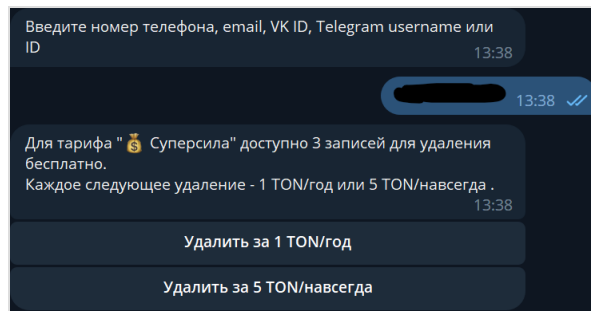
Скрытие данных о себе из Telegram-бота Insight

Для скрытия данных о себе в боте Insight необходимо: - чтобы было не менее ₴1000 пополнений за всё время с аккаунта - обратиться в поддержку внутри бота с просьбой удалить свои данные

Скрытие данных о себе из Telegram-бота GTA

Для скрытия данных о себе в боте GTA (Global Tech Aggregator) необходимо: - запускаем бот - “Мой аккаунт” - “Удалить информацию” - “Удалить запись” - по отдельности вводим интересующие идентификаторы - пополняем кошелек в TON (для удаления на год - 1 TON, навсегда - 5 TON за 1 идентификатор)





Удаление данных о себе из Telegram-бота Zernenda

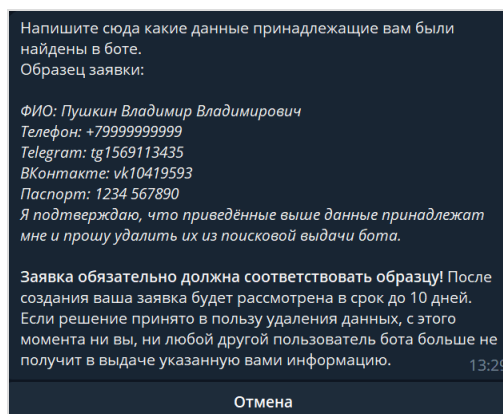
Для удаления данных о себе в боте Zernenda необходимо: - запускаем бот, подтверждаем аккаунт - проверяем какие данные о вас знает бот и из каких утечек (для этого оплачиваем несколько запросов по номеру телефона, ФИО и т.д.; выписываем себе, какие данные нашел бот) - “Мой аккаунт” - “Удалить данные о себе” - отправить свой номер телефона для подтверждения аккаунта - отправить подробную заявку с указанием того, какие данные вам принадлежат

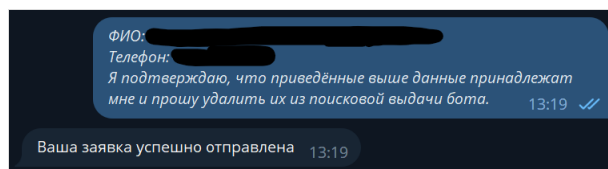
Образец заявки:

ФИО: Пушкин Владимир Владимирович Телефон: +79999999999

Telegram: tg1569113435 ВКонтakte: vk10419593 Паспорт: 1234 567890

Я подтверждаю, что приведённые выше данные принадлежат мне и прошу удалить их из поисковой выдачи бота.





Удаление данных о себе из Telegram-бота Архангел

Для удаления данных о себе в боте Архангел необходимо: - запускаем бот - “Профиль” - “Приобрести запросы” - покупаем запросы (требуется вариант “800 запросов - 5760 руб.”) - запускаем бот:

<https://t.me/AngelSystemSupportBot> - пишем “Пополнил на 800 запросов. Прошу удалить мои данные из вашей системы (надо написать, какие именно данные – телефон, почты, соцсети, документы, адреса и т.д.)”



Удаление данных о себе из Telegram-бота Cerberus

Для удаления данных о себе в боте Cerberus необходимо: - запускаем бот - “Аккаунт” - “Защитить данные” - “Создать” - По очереди вводим данные, которые предлагают ввести

Отключение поиска данных о своём номере в GetContact

В GetContact возможно произвольно отключить отображение имён, которые известны по вашему номеру, либо отключить поиск совсем.

Чтобы сделать это, надо перейти по этой ссылке и авторизоваться через мессенджер, затем выключить.

Также надо отметить, что в этом разделе сайта можно отслеживать поисковые запросы по вашему номеру. При отключении поиска эта возможность теряется так же как и получение уведомлений о поиске вас из приложения. Однако, при повторном входе в приложение GetContact эта возможность возвращается.

Visibility Settings

Visibility settings 

You don't want to appear in search results? We would like to share with you some tips that may affect your decision.

By unlisting from search results, you won't be able to do the following:

* Enterprises, banks or similar business corporations and individuals may want to see the person they do business with in Getcontact in order to know them better. Not being visible in Getcontact may result in worries in such cases.

* You won't be notified when your phone number is searched by other Getcontact users.

* You will not be able to see the tags other Getcontact users will create for you in the future.



Search visibility: On

Are you sure you want to unlist from search results?

Please note that it can take up to 3 hours before changes take effect and your phone number will be visible again in search results when you start to use Getcontact with the same number.

No

Yes

Раздел будет дополняться

Если ни одна из описанных процедур не подходит вашему случаю — например, данные всплывают там, где процедуры удаления нет вовсе, — можно разобрать ситуацию отдельно: counter-osint+book@soxoj.com.

Демонстрация экрана

В постковидное время удалённая работа стала нормой. Много людей созваниваются с коллегами в специально предназначенных для этого приложениях: Zoom, Microsoft Teams, Google Meet и так далее. Одним из неотъемлемых атрибутов таких приложений является функция демонстрации вашего экрана: чтобы показать собеседнику что-то, вы делаете видимым ваш рабочий стол или отдельные окна, например, браузер.

Разумеется, это несёт с собой и риски раскрытия чувствительной информации. Оставим в стороне факт целенаправленного показа вами чего-то, рассмотрим только случайные последствия:

- Переписки и сообщения в мессенджерах и соцсетях (во всплывающих окнах)
- Открытые вкладки в браузере или закладки
- Подсказки автодополнения во всех окнах ввода (особенно в адресной строке браузера)

Последняя категория может нести наибольший риск: при посимвольном вводе браузер будет пытаться предложить вам что-то из истории недавнего посещения, поисковых запросов или закладок, имеющее хоть какое-то совпадение с символами (даже если это похожие буквы в любом месте).

Чтобы отключить это поведение, на Firefox можно снять все галочки в разделах “Поиск / Поисковые предложения” и “Приватность и Защита / Панель адреса”.

Поисковые предложения
Выберите, где будут появляться предложения от поисковых систем.
☐ Отображать поисковые предложения
☐ Отображать поисковые предложения при использовании панели адреса
☐ Отображать поисковые предложения перед историей веб-сёрфинга при использовании панели адреса
☐ Отображать поисковые предложения в приватных окнах
[Изменить другие настройки предложений в адресной строке](#)

Панель адреса

При использовании панели адреса предлагать ссылки

- ☐ из журнала посещений
- ☐ из закладок
- ☐ из открытых вкладок
- ☐ из ярлыков
- ☐ из поисковых систем

Россия

Раздел будет дополняться

Документы

Все приведённые ниже идентификаторы можно использовать для поиска владельца.

Физические лица

- **Номер паспорта**
- **СНИЛС** - *страховой номер индивидуального лицевого счёта*
- **ИНН** - *идентификационный номер налогоплательщика*
- **УИН** - *уникальный идентификатор начислений*

Юридические лица

- **ОГРН** - *основной государственный регистрационный номер*

Транспорт

- **Номер автомобиля**
- **Номер полиса ОСАГО** - *обязательное страхование гражданской ответственности*
- **Номер СТС** - *свидетельство о регистрации транспортного средства*
- **ВУ** - *водительское удостоверение*

Главный государственный сервис - Госуслуги. Возможно восстановление доступа через любой из первых трёх документов физического лица, при этом раскроется часть вашего мобильного телефона или почты. Не рекомендуется вносить СНИЛС или ИНН в личный кабинет без явной необходимости.

Пробив

Какие услуги по получению данных через сотрудников доступны в России?

- Данные от мобильных операторов: Билайн, Мегафон, МТС.
Детализация звонков, местоположение (так называемая “Вспышка”).

- ПФР (*Пенсионный фонд России*). СНИЛС, выписка с лицевого счета застрахованного лица (СЗИ-6), дата смерти, актуальное место работы, материнский капитал.
- МВД (*Министерство внутренних дел*). Базы ИБД-Р, ИБД-Ф, Роспаспорт, Поток, Мигрант, Магистраль, Рубеж.
- ГИБДД (подразделение МВД). Карточки, штрафы, ограничения, список авто, карты ТС (транспортных средств), ВУ.
- ФНС (*Федеральная налоговая служба*). СНИЛС, счета, ЕГРН, ЕГРЮЛ, 2НДФЛ, книги покупки и продажи, архивная выписка, декларация, аффилированность, страховые взносы, задолженности.

Утечки данных в публичный доступ

В декабре 2021 года произошла утечка программного кода регионального сайта Госуслуг. Федеральный сайт не был затронут, но вероятность утечки данных с него существует.

В феврале 2022 года произошла утечка базы доставки Яндекс.Еды. Были опубликованы *имена и фамилии клиентов, номера телефонов, полный адрес доставки клиента и комментарии к заказу*. Всего почти 7 миллионов уникальных номеров из РФ и Казахстана, даты с 19.06.2021 по 04.02.2022. Для проверки своих данных энтузиастами был поднят сервис <https://saverudata.info/>.

Другие утечки

- ФОМС - *фонд обязательного медицинского страхования*
- УФМС
- ПФР
- СНИЛСы граждан

Украина

Раздел будет дополняться

Документы

Все приведённые ниже идентификаторы можно использовать для поиска владельца.

Физические лица

- **Номер паспорта**
- ДРФО - *идентификационный номер физического лица*
- РНОКПП (ІПН) - *регистрационный номер учетной карточки налогоплательщика*
- ВУ - *водительское удостоверение*

Государственные сервисы: - Дія - электронный сервис государственных услуг

Юридические лица

- ЕДРПОУ - номер в едином государственном реестре предприятий и организаций Украины

Пробив

Раздел будет дополняться

Утечки данных в публичный доступ

В январе 2022 года появилась информация об утечке базы сервиса Дія. Несмотря на заверения властей о том, что утечка фальшивая, энтузиастами было подтверждено её происхождение.

Проверить факт утечки ваших данных из сервиса можно здесь.

Беларусь

Раздел будет дополняться

Документы

Все приведённые ниже идентификаторы можно использовать для поиска владельца.

Физические лица

- УНП - *учётный номер плательщика*

Пробив

Раздел будет дополняться

Утечки данных в публичный доступ

В 2021 было хакеры заявили о получении доступа к АИС “ГАИ-Центр”, АИС “Паспорт”, к базе УСБ и “Беспорядки” МВД Беларуси, а также о взломе БД сотрудников СК Беларуси. В публичном доступе были выложены только некоторые данные, но журналистам также предоставили возможность проверить персональные данные конкретных людей и проанализировать массив персональных данных 1.4 миллиона умерших жителей.

В феврале 2022 года произошла утечка базы доставки Яндекс.Еды. Были опубликованы *имена и фамилии клиентов, номера телефонов, полный адрес доставки клиента и комментарии к заказу*. Всего 206 тысяч уникальных номеров из Беларуси, даты с 19.06.2021 по 04.02.2022. Для проверки своих данных энтузиастами был поднят сервис <https://saverudata.info/>.

Казахстан

Раздел будет дополняться

Документы

Все приведённые ниже идентификаторы можно использовать для поиска владельца.

Физические лица

- ИИН - *индивидуальный идентификационный номер*
- РНН - *регистрационный номер налогоплательщика*

Юридические лица

- БИН - *бизнес-идентификационный номер*

Транспорт

- ГРНЗ - *государственный регистрационный номерной знак*
- СРТС - *свидетельство о регистрации транспортного средства*

Главный государственный сервис - Электронное правительство республики Казахстан.

Пробив

Раздел будет дополняться

Утечки данных в публичный доступ

Летом 2019 года во время президентских выборов произошла утечка персональных данных 11 миллионов казахстанцев из ЦИК (Центральной избирательной комиссии).

В феврале 2022 года произошла утечка базы доставки Яндекс.Еды. Были опубликованы *имена и фамилии клиентов, номера телефонов, полный адрес доставки клиента и комментарии к заказу*. Всего почти 7 миллионов уникальных номеров из РФ и Казахстана, даты с 19.06.2021 по 04.02.2022. Для проверки своих данных энтузиастами был поднят сервис <https://saverudata.info/>.

Документы, удостоверяющие личность, в Бразилии: что это и для чего они нужны

Бразилия с населением более 210 миллионов человек, распределённым по 26 штатам и федеральному округу, использует различные идентификационные документы — для идентификации граждан и организаций, а также для реализации их прав и обязанностей. Эти документы различаются по назначению, сфере применения и сроку действия.

CPF — индивидуальный номер налогоплательщика

CPF — ключевой документ для идентификации в Федеральной налоговой службе Бразилии, ведомстве, отвечающем за федеральные налоги. Номер состоит из 11 цифр, включая две контрольные. CPF обязателен для всех бразильцев и иностранцев, проживающих в стране, и требуется для широкого круга финансовых операций: открытия банковских счетов, получения кредитов, подачи налоговых деклараций.

Кроме того, CPF необходим для доступа к социальным программам (например, Bolsa Família), участия в государственных экзаменах и отборах, а также для поступления в учебные заведения. Номер CPF может быть напечатан на удостоверении личности или на национальном водительском удостоверении.

RG — общий регистр

RG — удостоверение личности, выдаваемое органами общественной безопасности штатов. Состоит из порядкового номера и аббревиатуры штата, его выдавшего. RG содержит такие сведения, как имя, дату рождения, данные о родителях, фотографию, подпись и отпечаток пальца владельца. Помимо функции удостоверения личности, RG действует на всей территории страны и может использоваться как документ для поездок в странах МЕРКОСУР.

Важно отметить, что RG часто требуется при открытии банковских счетов, получении официальных документов и участии в государственных экзаменах. Получение RG также связано с обязательной воинской регистрацией для мужчин старше 18 лет.

CNPJ — национальный реестр юридических лиц

CNPJ — документ, идентифицирующий компанию в Федеральной налоговой службе Бразилии. Состоит из 14 цифр, включая две контрольные. CNPJ содержит такие сведения, как полное наименование, торговое наименование, адрес, вид экономической деятельности и размер уставного капитала.

Для компаний CNPJ необходим для ведения коммерческой деятельности, выставления счетов, найма сотрудников и исполнения налоговых обязательств. Кроме того, он используется для получения кредитов, открытия корпоративных банковских счетов и участия в государственных тендерах. Номер CNPJ может быть напечатан на разрешении на деятельность или на карточке *Simples Nacional*.

RENAVAM — национальный реестр транспортных средств

RENAVAM — документ, идентифицирующий транспортное средство в Национальном департаменте транспорта (*Denatran*), ведомстве, координирующем работу дорожных служб штатов. Состоит из 11 цифр и содержит сведения о марке, модели, годе выпуска, цвете, номерном знаке и номере шасси.

Помимо того, что RENAVAM обязателен для всех транспортных средств в эксплуатации, он необходим для перерегистрации авто, уплаты связанных с ним пошлин и налогов, ежегодного продления лицензии, а также для оформления таких процедур, как передача права собственности и смена муниципалитета регистрации.

Номер RENAVAM также указан в Свидетельстве о регистрации и лицензировании транспортного средства (*CRLV*) и доступен на портале *Denatran*.

CRV — свидетельство о регистрации транспортного средства

CRV — документ, подтверждающий право собственности на транспортное средство в Департаменте автотранспорта штата (*Detran*) по месту проживания владельца. Содержит те же сведения, что и

RENAVAM, и одновременно служит документом для передачи права собственности на ТС.

Помимо перечисленных функций, CRV необходим при купле-продаже автомобилей с пробегом, так как формализует передачу права собственности, обеспечивая регистрацию и законность сделки. Поэтому документ следует хранить в надёжном месте и не возить вместе с автомобилем.

Утечки данных: угроза приватности и безопасности

Вопросы безопасности данных актуальны во всём мире, и Бразилия не исключение: страна сталкивалась с инцидентами утечек чувствительной информации, способных серьёзно повлиять на приватность и безопасность её граждан.

Мегаутечка CPF: два года спустя вопросы по-прежнему без ответа

В январе 2021 года произошла крупнейшая утечка данных в истории Бразилии. Около 223 миллионов бразильских CPF оказались в свободном доступе на одном из интернет-форумов; хакер также продавал сведения об этих людях — адреса, телефоны, email, кредитный рейтинг, зарплату, доходы и многое другое.

Инструмента для проверки, попали ли ваши данные в этот дамп, не существует, и вряд ли такой инструмент появится. Верховный федеральный суд (STF) распорядился закрыть сайт «Fui Vazado», который позволял по номеру CPF проверять, какие именно данные о человеке фигурировали в мегаутечке.

Меры по повышению безопасности в Сети

Защита персональных данных в интернете критически важна для предотвращения мошенничества, кражи личных данных и других проблем. Вот меры, которые помогут повысить вашу онлайн-безопасность:

- **Управляйте паролями:** используйте сильные, уникальные и сложно угадываемые пароли для каждого сервиса. Периодически

меняйте их и никому не сообщайте. Используйте менеджер паролей для хранения и генерации надёжных паролей.

- **Не публикуйте чувствительные данные в соцсетях:** воздержитесь от публикации адреса, телефона, CPF, RG, сведений о доходах, местоположении и распорядке дня. Эти данные могут быть использованы злоумышленниками для выдачи себя за вас или для слежки. Настройте приватность в своих соцсетях.
- **Распознавайте и избегайте мошенничества:** не переходите по подозрительным ссылкам, не открывайте неизвестные вложения, не сообщайте личные данные на ненадёжных сайтах и в письмах. Многие схемы используют фишинг, чтобы обманом получить ваши данные или установить вредоносное ПО на устройство. Используйте антивирус и межсетевой экран.
- **Будьте осторожны при покупках онлайн:** совершайте покупки только на проверенных сайтах и убеждайтесь, что они используют протокол HTTPS (защищённое соединение). Избегайте ввода данных кредитных и дебетовых карт на неизвестных и подозрительных сайтах; используйте виртуальные карты или сервисы онлайн-платежей, чтобы не светить банковские данные.
- **Не доверяйте публичным сетям:** избегайте публичных Wi-Fi и общих компьютеров для работы с сервисами, требующими личных данных (почта, банкинг, соцсети). Такие сети могут прослушиваться или содержать вредоносное ПО. Если иначе нельзя — используйте VPN для шифрования трафика.

Защита данных и осознанное отношение к безопасности — основа цифровой эпохи, где персональная информация всё плотнее переплетена с повседневной жизнью. Проактивные меры безопасности в Сети помогают сохранить вашу приватность и защитить вас от возможных киберугроз.

Об этом издании

Книга собрана автоматически из исходного текста руководства, который ведётся в открытом репозитории. Содержание и опечатки правятся там же.

Издание от 30.10.2026.

Актуальная версия и другие форматы: counter-osint.soxoj.com/pdf

Если вы читаете устаревшую копию — по этому адресу всегда лежит свежая.