

Данные ПОД КОНТРОЛЕМ:

Как защитить личную информацию
в цифровом мире



и
Анна Инежина

Анна Инежина

Данные под контролем: Как защитить личную информацию в цифровом мире

<https://litres.ru/74627074>

SelfPub; 2026

Аннотация

Сказали коллеге о поездке — и наутро увидели рекламу отдыха. Телефон подслушивает? Не обязательно: поиски, геометки и разрешения приложений оставляют цифровой след, который легко недооценить.

«Данные под контролем» поможет понять, кто собирает ваши сведения, какие риски реальны и что стоит защищать в первую очередь. Выстройте защиту без паранойи: ограничьте доступ приложений, укрепите аккаунты уникальными паролями и вторым фактором, безопаснее будете хранить файлы и пользоваться сервисами. А если столкнётесь с мошенничеством, утечкой или взломом — будете знать, с чего начать. Для всех, кто пользуется смартфоном, покупает онлайн и делится информацией. Практичные шаги, чтобы личные данные оставались под вашим контролем.

Книга создана с помощью ИИ. Обложка: GPT Image -
Лицензия

Содержание

Личный цифровой след: какие данные о вас собираются и как используются	6
Модель угроз: от чего защищаться, кому доверять и что важнее всего сохранить	20
Основы цифровой защиты: минимизация данных, разделение и контроль доступа	31
Аккаунты под защитой: уникальные пароли, менеджеры паролей и многофакторная аутентификация	42
Конец ознакомительного фрагмента.	50

Анна Инежина

Данные под контролем:

Как защитить личную

информацию в

цифровом мире

Данные под контролем: Как защитить личную информацию в цифровом мире

Анна Инежина

Личный цифровой след: какие данные о вас собираются и как используются

Вечером Лена сказала коллеге за кофе:

— Кажется, в июне всё-таки поеду в Карелию. Хочу несколько дней провести у воды, без расписания и толпы.

На следующий день в ленте появилась реклама домика у озера. Лена нахмурилась. Она не искала домики, не отправляла коллегам ссылки и, насколько помнила, не вводила в телефон слово «Карелия».

Самое простое объяснение пришло первым: телефон подслушивал разговор. Но совпадение — ещё не доказательство. Возможно, Лена незадолго до этого искала расписание поездов или смотрела фотографии северных озёр. Возможно, она разрешила приложению доступ к геолокации, а рекламный сервис связал её поездки с интересом к путешествиям. Возможно, она входит в группу людей с похожими привычками: они читают те же сайты, бывают в тех же местах и покупают похожие товары. Или объявление увидели многие, а внимание зацепилось именно за то, что совпало с разговором.

Рекламные системы обычно не нуждаются в мистике. Им хватает множества небольших наблюдений, каждое из кото-

рых по отдельности кажется пустяком. Вместе они складываются в биографию — не обязательно точную, не обязательно справедливую, но достаточно убедительную, чтобы подобрать объявление.

Чтобы понять, откуда эта биография берётся, проследим за одним обычным днём.

Один день — десятки следов

В 7:10 Лена выключает будильник и открывает приложение погоды. Телефон уже знает, что он включён, подключён к сети и использует определённую версию операционной системы. Приложение может получить технические сведения об устройстве, а при наличии разрешения — доступ к примерному или точному местоположению. Погодному сервису нужно понять, для какого района показать прогноз. Но для этого не всегда нужны точные координаты: иногда достаточно выбранного вручную города или приблизительной оценки по интернет-адресу устройства.

Через десять минут Лена строит маршрут до офиса. Навигационное приложение получает запрос, который включает начальную и конечную точки, время и выбранный способ передвижения. Если включена история местоположений, сервис может сохранять посещённые места или маршруты. Если выключена — приложение всё равно может обрабатывать текущие координаты, пока строит путь. Это разные действия: запрет на долговременное сохранение не всегда означает, что данные вообще не используются.

По дороге Лена покупает кофе и платит телефоном. В самой кофейне остаётся запись о покупке: время, сумма, место, а иногда и состав заказа — если он указан в чеке или приложении лояльности. Платёжный посредник обрабатывает транзакцию; банк видит её в выписке; кофейня может связать покупку с аккаунтом, если Лена предъявила карту лояльности или заказала через приложение. Каждый участник видит свою часть истории.

В обед Лена ищет билеты на поезд. Поисковая система получает запрос. Сайт перевозчика может сохранить сведения о маршруте, датах, выбранном тарифе и покупке. Если Лена вошла в аккаунт, поездка будет связана с ним напрямую. Если не вошла, сайт всё равно может временно распознавать её браузер по файлам cookie, техническим характеристикам устройства или другим идентификаторам. Не каждый сервис использует все эти способы и не каждый идентификатор позволяет узнать имя человека. Но он может помочь отличить одно устройство или браузер от другого, а затем сопоставить действия.

После работы Лена отправляет подруге фотографию набережной. На снимке может быть не только изображение. В файле иногда сохраняются дата, время и координаты съёмки. Приложение для переписки может передавать фотографию иначе, чем камера её сохранила: например, сжать её или удалить часть метаданных. Социальная сеть может дополнительно распознать место по содержимому кадра, сопоставить

его с отметкой геолокации или связать публикацию с профилем Лены. А друзья, которые увидели фотографию, тоже становятся частью истории: кто-то может отметить её на снимке, переслать его или оставить комментарий.

Так выглядит карта одного условного дня. Она не означает, что каждый сервис собирает всё перечисленное. Это перечень вопросов, которые стоит задать конкретному приложению или компании.

Источник данных

Возможный получатель

Возможная цель

Срок хранения

Возможность отказаться

Запрос маршрута и координаты

Навигационный сервис, поставщик карт

Построить маршрут, оценить пробки, улучшить сервис

Текущий запрос, журналы событий или история аккаунта

— зависит от настроек и правил сервиса

Ограничить доступ к геолокации, отключить историю, удалить сохранённые места; навигация может стать менее точной

Данные о покупке кофе

Кофейня, платёжная система, банк

Провести платёж, учесть покупку, начислить бонусы, вести бухгалтерский учёт

Зависит от участника; финансовые записи могут храниться дольше маркетинговых данных

Не участвовать в программе лояльности, не создавать аккаунт; отказаться от отдельных рекламных сообщений

Поисковые запросы и посещение сайта

Поисковик, сайт, рекламные или аналитические партнёры

Ответить на запрос, измерить посещаемость, показать рекламу

Может зависеть от аккаунта, cookie и настроек; сроки различаются

Использовать настройки истории и cookie, блокировать необязательный трекинг, где это доступно

Покупка билета

Перевозчик, платёжный посредник, банк

Оформить поездку, оплатить её, выполнить требования учёта и безопасности

По правилам перевозчика и финансовым требованиям

Без аккаунта можно сократить привязку к профилю, но не отменить данные, необходимые для самой поездки

Фотография и отметка места

Социальная сеть, сервис хранения, подписчики

Показать публикацию, сохранить фото, подобрать контент и рекламу

До удаления, согласно настройкам и правилам; копии у других людей могут сохраниться

Не публиковать, убрать геометку, ограничить аудиторию, удалить публикацию; уже сделанные копии контролировать трудно

Сведения с телефона и приложений

Производитель платформы, разработчики приложений, аналитические службы

Обеспечить работу, защиту, диагностику и измерение использования

От короткого срока для журналов до периода жизни аккаунта — зависит от данных и сервиса

Проверить разрешения, сбросить рекламные настройки, отключить необязательную диагностику, удалить неиспользуемое приложение

Главное слово в таблице — «возможный». Условия зависят от страны, сервиса, настроек и типа информации. Если точный срок хранения не указан, его не нужно угадывать. Это отдельный вопрос компании: что именно хранится, для чего, как долго и можно ли удалить данные. А если вы отказываетесь от персонализированной рекламы, это не всегда прекращает сбор данных. Иногда меняется только способ их

использования: сервис перестаёт подбирать объявление под ваш профиль, но продолжает собирать сведения, необходимые для работы или измерения посещаемости.

Данные, метаданные и выводы

Чтобы читать цифровой след, полезно различать три слоя.

Данные о содержании — это то, что человек сообщает непосредственно: текст письма, фотография, комментарий, заполненная анкета, поисковый запрос. Сюда же относятся сведения, которые вы публикуете сами: место работы в профиле, фотография с мероприятия, рассказ о покупке.

Метаданные — сведения об обстоятельствах, в которых появилась информация. Для сообщения это могут быть время отправки, адресаты и устройство; для фотографии — дата съёмки и, если сохранены, координаты; для посещения сайта — время, длительность и тип браузера. Метаданные часто не содержат самого разговора или изображения, но способны многое рассказать о ритме жизни. Например, регулярные посещения одного адреса в будние дни могут указывать на рабочий маршрут.

Выводы — предположения, которые система строит на основе наблюдений. Если человек регулярно читает статьи о беговых кроссовках, сервис может предположить интерес к спорту. Если он ищет билеты и открывает страницы жилья, система может отнести его к аудитории путешественников. Вывод не равен факту: интерес к статье о беременности не доказывает, что человек ждёт ребёнка; поиск ле-

карств не устанавливает диагноз. Но даже ошибочный вывод может повлиять на то, какую рекламу, цену, рекомендацию или контент человек увидит.

Отдельные следы становятся значимее, когда их сопоставляют. Одна покупка говорит мало. История покупок, мест и поисков может обозначить привычки. Идентификатор устройства или аккаунт помогает системе связать некоторые события между собой. Рекламные и аналитические компании могут получать данные от разных источников, однако набор доступных им сведений неодинаков и зависит от настроек, договоров и правил конкретных сервисов. Не следует представлять это как единую базу, где кто-то видит каждое действие каждого человека. Полезнее задавать практический вопрос: **кто именно получает эти сведения и с какой целью?**

Четыре этапа одной истории

Управлять данными легче, если не смешивать разные этапы их жизни.

1. Сбор. Сайт записывает, какие страницы вы открыли; приложение запрашивает контакты; магазин получает сведения о заказе. Сбор может быть необходим для функции, которую вы используете, или относиться к дополнительной аналитике и рекламе.

2. Хранение. Данные остаются в аккаунте, журнале событий, резервной копии или системе учёта. У разных сведений — разные сроки. Маршрут может быть нужен несколько

минут, историю заказов компания хранит для обслуживания покупки, а финансовые записи — дольше по требованиям закона.

3. Сопоставление. Сервис связывает события с аккаунтом, устройством, номером карты лояльности или рекламным идентификатором. Иногда сопоставление происходит внутри одной компании, иногда данные передаются партнёрам. Чем больше устойчивых идентификаторов и связей, тем подробнее может быть профиль.

4. Использование. На основе данных сервис показывает рекламу, строит рекомендации, обнаруживает мошенничество, измеряет работу продукта или помогает выполнить заказ. Эти цели не равноценны: одни нужны, чтобы предоставить услугу, другие могут быть необязательными.

Именно поэтому настройка приватности редко сводится к одной кнопке. Можно запретить приложению постоянный доступ к геолокации, но оставить его возможность использовать координаты во время навигации. Можно отключить персонализацию рекламы, но продолжить получать объявления. Можно удалить историю из своего аккаунта, хотя у компании могут сохраняться отдельные записи по законным или техническим причинам. Важно понимать не только «собирают ли данные», но и на каком этапе вы хотите ограничить их.

Карта моего следа

Сейчас устройте короткую инвентаризацию. Не пытайтесь сразу перечислить каждое приложение и каждую строчку по-

литики конфиденциальности. Ваша задача — увидеть главные маршруты данных.

Шаг 1. Перечислите источники. Запишите устройства, которыми регулярно пользуетесь: телефон, компьютер, часы, телевизор, автомобильная система, умная колонка. Добавьте аккаунты и приложения: электронная почта, карты, магазины, соцсети, банк, облачное хранилище, сервисы здоровья, браузер.

Шаг 2. Отметьте категории сведений. Возле каждого источника укажите, что он может получать: имя и контакты; местоположение; поиски и просмотр страниц; покупки и платежи; фотографии и сообщения; голосовые команды; сведения о здоровье; технические данные устройства; список действий внутри приложения.

Шаг 3. Назовите получателя и цель. Не пишите просто «интернет». Уточните: сам разработчик приложения, магазин, платёжный посредник, производитель устройства, социальная сеть, рекламный партнёр. Если получатель неизвестен, поставьте вопросительный знак. Затем запишите вероятную цель: работа функции, доставка заказа, безопасность, аналитика, персонализация рекламы.

Шаг 4. Проверьте хранение и отказ. Откройте настройки приложения и найдите разрешения, историю, рекламные предпочтения, экспорт или удаление данных. В политике конфиденциальности ищите разделы о сроках хранения, партнёрах и целях обработки. Не обязательно читать

всё сразу: начните с сервисов, которые знают о вас больше всего. Запишите, что удаётся отключить, что можно удалить и что необходимо для предоставления услуги.

Для одного аккаунта это может выглядеть так:

Источник

Сведения

Получатель и цель

Что проверить

Приложение карт

Геолокация, маршруты, поиск мест

Сервис карт: навигация и, возможно, история поездок

Разрешение «при использовании», история мест, автосохранение

Магазин

Адрес, заказ, способ оплаты, история покупок

Магазин и платёжный посредник: исполнение заказа и расчёты

Гостевой заказ, маркетинговые согласия, удаление аккаунта

Социальная сеть

Публикации, реакции, контакты, данные устройства

Платформа: показ публикаций, рекомендации, безопас-

ность

Аудитория, синхронизация контактов, рекламные настройки

Умные часы

Активность, пульс или сон — если включены соответствующие функции

Производитель устройства и связанное приложение: статистика и здоровье

Какие показатели записываются, с кем делятся, как удалить историю

Карта не обязана быть полной. Даже три заполненные строки полезнее, чем тревожное ощущение, будто «все всё знают». Она показывает, где сведения действительно появляются и какое действие можно предпринять.

Чужие руки в вашей биографии

Не весь цифровой след создаёте вы. Друг может загрузить групповую фотографию и отметить вас. Сервис доставки хранит адрес, указанный для посылки. Контакт из телефонной книги может загрузить список номеров в приложение, чтобы найти знакомых; некоторые приложения предлагают такую функцию, но дают возможность не включать синхронизацию. Компания может получить адрес из договора или заказа, даже если вы ничего не публиковали в интернете.

Есть и след, который создают повседневные устройства

без заметного участия человека: журналы входа, сведения о сбоях, данные о соединении. Они помогают поддерживать работу и защищать аккаунты, но тоже заслуживают внимания. Чем меньше ненужных приложений и бессрочных разрешений, тем меньше мест, где накапливается история.

Это не повод стремиться к полной невидимости. Большинство людей пользуются цифровыми сервисами именно потому, что те помнят адрес доставки, находят маршрут и сохраняют фотографии. Цель — не отказаться от удобства, а различать необходимое и лишнее, понимать цену выбора и регулярно проверять, не изменились ли настройки.

Начните с простого перечня сведений, которыми стоит управлять:

- точная геолокация и история мест;
- доступ приложений к контактам, микрофону, камере и фотографиям;
- история поиска и просмотров, связанная с аккаунтом;
- платёжные данные, покупки и программы лояльности;
- публичность публикаций, отметки на фотографиях и геометки;
- синхронизация контактов и подключение сторонних аккаунтов;
- сроки хранения данных и настройки рекламной персонализации.

У каждого пункта свой баланс пользы и приватности. Геолокация нужна навигатору, но не обязательно фоновой игре.

Контакты могут помогать находить друзей, но не требуются приложению-фонарю. История покупок удобна для возврата товара, но рассылка предложений — отдельная цель. Разделяя эти решения, вы возвращаете себе не абсолютный контроль, а более важную вещь: осознанный выбор.

Цифровая биография складывается не только из того, что мы решаем рассказать. Её дополняют устройства, привычки, метаданные и действия других людей. Первый шаг к защите — не паника и не попытка исчезнуть, а карта: что возникает, где хранится, с чем связывается и как используется. Когда эта карта перед вами, становится легче решить, какие риски важны именно для вас — и от чего защищаться в первую очередь.

Модель угроз: от чего защищаться, кому доверять и что важнее всего сохранить

В половине второго ночи Алексей понял, что у него стало больше средств защиты, чем понимания. На телефоне стояли два приложения для шифрования, три браузера, VPN, блокировщик рекламы и программа, которая обещала «стереть цифровой след». Пароли он сменил не везде, резервные копии не проверял, а к почте по-прежнему привязывались все остальные аккаунты. Алексей старательно закрывал каждую дверь — и не знал, какие из них ведут к его дому.

Так часто начинается цифровая защита: с тревоги. В новостях крадут базы данных, знакомым взламывают мессенджеры, незнакомцы находят старые фотографии. В ответ хочется защищаться от всего и сразу. Но в цифровом мире нельзя запереть каждую дверь и при этом продолжать жить. Важно понять, какие двери ведут к тому, что для вас действительно ценно, и кто с наибольшей вероятностью попытается войти.

Именно для этого нужна модель угроз. Не список катастроф и не чертёж секретного бункера, а практичный способ принять несколько решений: что сохранить, от кого, каким способом и какой уровень защиты имеет смысл.

Не все данные одинаково важны

Представим журналистку-фрилансера Надю. Она пишет о муниципальных закупках и иногда общается с людьми, которые не хотят раскрывать свои имена. Для неё особенно важны переписка с источниками, черновики расследований и доступ к рабочей почте. Потеря телефона неприятна, но опаснее, если через него можно добраться до почты, облачного хранилища и личностей собеседников. А публикация номера телефона или адреса может создать уже не только цифровую проблему.

Теперь сравним Надю с родителем, который хранит семейные фотографии и управляет школьными аккаунтами ребёнка; со студентом, которому нужны материалы диплома и доступ к учебной почте; с владельцем небольшого магазина, у которого в таблице заказов записаны адреса клиентов. У каждого есть ценные данные, но ценность и последствия утраты различаются. Родителю важна доступность семейного архива, студенту — сохранность работы и учётной записи, предпринимателю — конфиденциальность клиентских сведений и возможность продолжать принимать заказы.

У Нади может быть выше вероятность целевой попытки получить конкретные материалы или установить личность источника. У родителя реалистичнее случайная утрата доступа к аккаунту или мошенничество с паролем. Владелец магазина стоит особенно думать о том, как защитить сведения клиентов и восстановить работу после поломки устройства. Это не соревнование, у кого опаснее жизнь. Это напо-

минание: защита должна соответствовать обстоятельствам.

Чтобы расставить приоритеты, полезно различать три свойства информации:

- **Конфиденциальность:** кто может её увидеть.
- **Целостность:** кто может её изменить или подменить.
- **Доступность:** сможете ли вы сами получить её тогда, когда понадобится.

Для журналистки конфиденциальность переписки с источником может быть критичной. Для студента важнее не потерять единственную копию диплома — здесь на первом месте доступность. Для магазина важны сразу все три свойства: нельзя раскрыть клиентские данные, потерять заказы или позволить кому-то незаметно изменить реквизиты оплаты.

К активам относятся не только файлы и сообщения. Это также учётные записи, устройства, способы восстановления доступа, контакты, история перемещений, деловая репутация и даже возможность доказать, что важный документ не был подменён.

Кто может быть противником

Слово «противник» звучит так, будто за каждым человеком следит профессиональная команда взломщиков. В модели угроз оно означает просто того, чьи действия способны причинить вред. Часто это не конкретная личность, а категория людей или событий.

Например:

- **Случайный мошенник** рассылает массовые письма и рассчитывает, что кто-то введёт пароль на поддельной странице.

- **Знакомый или бывший партнёр** может знать ответы на вопросы восстановления, иметь доступ к устройству или использовать общие аккаунты.

- **Злоумышленник, нацеленный на конкретного человека**, может подстраивать обман под его работу и круг общения.

- **Преступник, завладевший телефоном или ноутбуком**, получает возможность воспользоваться открытыми сессиями и сохранёнными данными.

- **Сервис или организация** могут собирать сведения, необходимые для работы продукта, а иногда — хранить их дольше или шире, чем вам хотелось бы.

- **Случайность** — поломка, потеря устройства, ошибка синхронизации — тоже способна лишить вас данных.

Важны не только намерения, но и возможности. Массовый мошенник, вероятно, не станет тратить недели на взлом одного малоизвестного аккаунта. Зато он может рассылать тысячи сообщений в надежде на одну удачу. Человек, который лично заинтересован в содержимом конкретного телефона, способен использовать знакомство с владельцем, его привычками и окружением.

Это помогает не впадать в две крайности. Первая: «Я никому не интересен, значит, защищаться не нужно». Вторая:

«Кто-то наверняка уже следит за мной, значит, никакие меры не помогут». Между ними находится разумный вопрос: **какая неприятность достаточно вероятна и достаточно серьёзна, чтобы я принял меры?**

Как возникает риск

Обычно атака — не волшебный взлом из фильма, а цепочка событий. Например, пароль от почты повторяется на нескольких сайтах. Один из сайтов теряет данные. Мошенник пробует тот же пароль в почте, входит в аккаунт, а затем запрашивает сброс паролей от других сервисов. Здесь слабое место не в том, что «интернет небезопасен», а в конкретной связке: повторный пароль, важная учётная запись и возможность восстановить через неё остальные.

У Нади может быть другой путь: правдоподобное сообщение якобы от редактора ведёт на поддельную страницу входа. Если она введёт пароль, атакующий попытается использовать полученный доступ. Защита должна учитывать не абстрактное «взломают», а этот маршрут: почта и переписка — ценная цель; сообщение может выглядеть убедительно; последствия затронут и её, и собеседников.

При оценке риска полезно задавать три вопроса:

1. Насколько вероятен сценарий? Есть ли у предполагаемого злоумышленника причина и простой способ действовать? Было ли что-то подобное раньше?

2. Насколько серьёзны последствия? Потеря одного вечера, финансовый ущерб, раскрытие частной информа-

ции, угроза работе или безопасности?

3. Насколько трудно снизить риск? Иногда небольшая мера — уникальный пароль или резервная копия — предотвращает много неприятностей. Иногда дополнительная защита сложна, мешает работе и даёт мало пользы.

Не нужно изображать математическую точность там, где её нет. Умножение «вероятности на ущерб» может помочь мыслить, но не превращает личную оценку в научный прогноз. Достаточно пометить риск как низкий, средний или высокий и объяснить себе почему. Если сценарий маловероятен, но последствия катастрофические, его всё равно стоит обдумать. Если событие вероятно, но легко обратимо, можно начать с простого способа восстановления.

Одностраничная модель угроз

Попробуем заполнить модель для Нади. Необходимо описать актив, вероятного противника, путь атаки, последствия, меру защиты и остаточный риск — то, что останется даже после принятых мер.

Актив

Возможный противник

Путь атаки

Последствия

Мера защиты

Остаточный риск

Переписка с источниками и рабочая почта

Массовый мошенник или человек, нацеленный на журна-
листку

Поддельное письмо приводит к краже пароля; доступ к
почте открывает другие аккаунты

Раскрытие личности собеседника, потеря материалов, за-
хват связанных аккаунтов

Уникальный длинный пароль в менеджере паролей; мно-
гофакторная аутентификация, по возможности — устойчи-
вый к фишингу способ; проверка адреса входа; резервный
способ восстановления

Устройство может быть разблокировано посторонним; ис-
точник может не защитить собственный аккаунт; провайдер
сохраняет часть метаданных

В этой строке видно, почему одной меры недостаточно.
Уникальный пароль снижает риск повторного использова-
ния, но не обязательно защитит от поддельной страницы
входа. Дополнительный фактор входа помогает, но не спа-
сает, если кто-то уже получил доступ к разблокированному
устройству. Защита источника зависит не только от Нади: со-
беседник может переслать переписку, потерять телефон или
назвать имя в разговоре с другим человеком.

Для собственной версии можно пройти шесть шагов.

1. Назовите актив. Не «вся моя приватность», а, на-
пример, «доступ к почте», «архив семейных фотографий»,

«список клиентов», «переписка с врачом».

2. Определите возможного противника. Выберите правдоподобную категорию, не придумывая всемогущего врага.

3. Опишите путь атаки. Как именно данные могут быть раскрыты, изменены, потеряны или заблокированы?

4. Запишите последствия. Что изменится для вас и других людей, если это произойдёт?

5. Выберите меру защиты. Начните с доступных действий, которые уменьшают наиболее важный риск.

6. Признайте остаточный риск. Что не исчезнет после защиты и с чем вы готовы жить?

Рассмотрим семейные фотографии. Актив — не только снимки, но и доступ к облачной учётной записи. Возможные причины потери — забытый пароль, мошенническое сообщение, поломка телефона или случайное удаление. Последствие — утрата единственной копии. Разумная мера — отдельная резервная копия, которую можно восстановить, и проверка, что фотографии действительно открываются. Остаточный риск остаётся: резервный диск может сломаться, аккаунт — быть захвачен. Но риск уже не сводится к одной хрупкой точке.

Доверие не исчезает — оно распределяется

Защищая данные, мы всё равно кому-то доверяем. Производитель устройства отвечает за обновления и часть встроенных механизмов безопасности. Операционная система

управляет доступом приложений. Облачный сервис хранит файлы и обеспечивает синхронизацию. Оператор связи участвует в доставке сообщений и иногда — в восстановлении доступа к номеру. А люди вокруг могут увидеть экран, переслать вложение или раскрыть информацию в разговоре.

Доверие — не переключатель «включено/выключено», а набор вопросов. Кто способен увидеть содержимое? Кто может восстановить доступ? Кто хранит резервные копии? Кто может заблокировать учётную запись? Какие сведения останутся даже при защищённом содержимом?

Например, сквозное шифрование в мессенджере обычно предназначено для того, чтобы содержание переписки могли прочитать участники, а не сам сервис при обычной передаче сообщений. Но оно не защищает сообщение на уже разблокированном телефоне и не гарантирует, что резервная копия настроена так же. Кроме того, могут оставаться сведения о взаимодействиях — например, время или факт соединения, в зависимости от сервиса и его настроек. Значит, важно смотреть не на одно обещание «зашифровано», а на весь путь данных.

Именно поэтому в модели угроз есть место людям, устройствам и компаниям. Иногда разумнее не передавать сервису лишние сведения. Иногда — выбрать надёжный способ восстановления доступа. Иногда — договориться с близкими, что фотографии ребёнка нельзя публиковать без согласия. Никакая программа не отменяет решений, которые

принимают люди.

Защищайте важное, а не воображаемое

Если бы Алексей начал не с установки приложений, а с модели угроз, возможно, он сперва укрепил бы почту, придумал уникальные пароли, включил дополнительную проверку входа и убедился, что умеет восстановить фотографии. Это не так эффектно, как скачать ещё один инструмент. Зато защищает конкретные вещи от реалистичных неприятностей.

Попробуйте потратить на свою модель двадцать минут. Выберите три актива, потеря или раскрытие которых действительно повлияли бы на вашу жизнь. Для каждого запишите наиболее правдоподобный путь неприятности, возможные последствия и одну меру, которую можно выполнить на этой неделе. Не пытайтесь охватить всё сразу. И не записывайте в таблицу сами пароли, секретные ключи или подробности, которые станут уязвимостью, если попадут не туда.

Хорошая модель угроз не обещает абсолютной безопасности. Её задача скромнее и полезнее: помочь потратить силы там, где они принесут наибольшую пользу. Она превращает тревожное «со мной может случиться что угодно» в ясное «вот что я хочу сохранить, вот чего опасаясь, вот что я могу сделать». Когда приоритеты определены, следующим шагом становится повседневная практика: собирать меньше данных, разделять личное и рабочее и выдавать каждому до-

ступ только к тому, что ему действительно необходимо.

Основы цифровой защиты: минимизация данных, разделение и контроль доступа

Марина регистрировалась на сервисе скидок между остановкой и офисом. Он обещал напоминать о распродажах рядом и начислить бонус ко дню рождения. На экране одно за другим появлялись поля: дата рождения, контакты, местоположение. Внизу — большая кнопка «Продолжить через аккаунт соцсети». Марина заполнила всё: так было быстрее, да и скрывать, казалось, нечего.

Через несколько месяцев сервис сообщил об инциденте безопасности. В уведомлении перечислялись сведения, которых коснулась утечка: адрес электронной почты, дата рождения, загруженная адресная книга и история местоположений. Пароли, уверяла компания, не пострадали. Но Марина вдруг увидела не просто набор записей, а кусочки своей жизни, которые сама сложила в чужую систему. Теперь ей приходилось менять настройки, предупреждать знакомых о возможных подозрительных сообщениях и гадать, куда еще разошлись данные.

Сервис не обязательно собирал их со злым умыслом. Дата рождения могла быть нужна для бонуса, контакты — чтобы находить друзей, геолокация — для предложений поблизо-

сти, а вход через соцсеть — для быстрого создания аккаунта. Но «может быть полезно» и «без этого нельзя» — не одно и то же. В цифровой защите часто важнее не отыскать идеальный инструмент, а не отдавать лишнее по привычке.

Три принципа, которые работают вместе

Уменьшить последствия цифрового инцидента помогают три простые идеи: собирать меньше данных, разделять контексты и выдавать доступ только в необходимом объёме. Они не гарантируют полной безопасности. Зато делают цифровую жизнь менее хрупкой: если одна часть системы даст сбой, под угрозой окажется меньше всего остального.

1. Собирать меньше

Минимизация данных — это не отказ от технологий и не попытка стать невидимым. Это привычка спрашивать: «Что действительно необходимо для этой задачи?» Если ответ — только адрес электронной почты, дата рождения и адресная книга могут остаться за пределами формы.

У этого принципа есть и инженерная логика: чем меньше данных хранится, тем меньше потенциальных сведений может оказаться затронуто при ошибке, утечке или неправомерном доступе. В европейском законодательстве о защите данных принцип минимизации сформулирован как требование собирать сведения, необходимые для конкретной цели, а не «на всякий случай». Это полезное правило и за пределами юридических формулировок.

При этом отдельные факты, которые кажутся безобидны-

ми, могут становиться значимее в сочетании. Дата рождения, город, должность, список знакомых и расписание поездов по отдельности не рассказывают о человеке всё. Вместе они могут помочь составить более точный профиль или сделать мошенническое сообщение убедительнее. Чем меньше ненужных кусочков вы оставляете в разных местах, тем труднее сложить из них подробную картину.

Минимизация — не обязательно «не указывать ничего». Важно соотнести сведения с задачей:

- Сервису с возрастными ограничениями может понадобиться подтвердить, что пользователь достиг нужного возраста. Но не каждому магазину нужен полный день, месяц и год рождения.
- Доставка товара требует адреса доставки, но не обязательно доступа к контактам телефона.
- Карте или приложению такси нужно местоположение для работы конкретной функции. Это не означает, что приложению нужна геолокация всегда.
- Сервису для общения могут быть нужны контакты, чтобы искать знакомых. Но если вы не пользуетесь этой функцией, разрешение можно не выдавать.

Не подменяйте минимизацию ложными данными там, где сведения важны для договора, платежа, безопасности или закона. Для финансового сервиса, медицинской записи или доставки точность может быть необходима. В остальных случаях разумно сначала выяснить, обязательны ли поля и что

именно перестанет работать без них.

2. Разделять контексты

Представьте дом, в котором все ключи открывают все двери. Если один ключ потерян, проблема затрагивает спальню, кабинет и кладовую сразу. Разделение цифровых контекстов работает как отдельные замки: оно не делает взлом невозможным, но ограничивает распространение последствий.

Начать можно с электронной почты. Один адрес удобно использовать для работы и важных аккаунтов, другой — для покупок, рассылок и скидочных программ. Если адрес для покупок попадёт в рекламные списки или начнёт получать подозрительные письма, это не обязательно потянет за собой переписку с врачом, банком или работодателем. Не нужно заводить десятки ящиков: разделение должно оставаться удобным, иначе оно быстро превратится в забытые пароли и хаос. Достаточно нескольких понятных категорий.

Так же полезно отделять рабочую жизнь от личной. Рабочие документы — в одобренном работодателем хранилище, личные фотографии — в личном аккаунте. Не стоит пересылать рабочие файлы на домашнюю почту «на минутку» или подключать личное облако к рабочему устройству без необходимости. Организация может управлять рабочими устройствами и данными по своим правилам; личный аккаунт в такой системе создает путаницу и для сотрудника, и для работодателя.

Разделение помогает и при покупках. Адрес для зака-

зов можно не использовать для регистрации на каждом новом форуме; отдельный профиль браузера позволяет не смешивать рабочие вкладки, личную почту и временные поиски подарка. Это не гарантирует анонимности. Платежи, номер телефона, устройство, привычки и сетевые данные могут связывать разные аккаунты между собой. Разделение — это способ уменьшить случайные связи и локализовать последствия, а не плащ-невидимка.

Проверка проста: если один аккаунт или сервис окажется скомпрометирован, какие другие сферы жизни он откроет? Если ответ — «почти все», контексты слишком тесно сцеплены.

3. Ограничивать доступ

Принцип наименьших привилегий звучит строго, но смысл у него бытовой: человеку, приложению или аккаунту следует давать только те права, которые нужны для конкретной задачи, и не больше.

Например, приложение для обработки фотографий просит доступ ко всей медиатеке. На многих устройствах можно выбрать только несколько снимков или воспользоваться встроенным системным окном выбора. Если приложение нужно для одной фотографии, доступ ко всему архиву — избыточный. Можно также проверить, нужен ли приложению доступ к точной геолокации, микрофону, камере и уведомлениям. Разрешение не обязано быть вечным: иногда достаточно варианта «только во время использования».

Для общего домашнего планшета лучше создать гостевую или отдельную пользовательскую учётную запись, а не передавать всем один профиль с открытой почтой, облаком и платёжными данными. Гость сможет пользоваться нужными функциями, не получая доступ ко всему остальному. В семье похожий принцип применим к подпискам и хранилищам: удобнее пригласить близкого в семейную группу с нужными правами, чем сообщать ему пароль от своего аккаунта.

С файлами действует та же логика. Если коллеге нужно прочитать документ, предоставьте просмотр, а не редактирование. Если ссылка нужна на один проект, не открывайте целую папку. Для чувствительных материалов полезны срок действия ссылки и возможность отозвать доступ. Эти настройки не заменяют осторожность: получатель всё ещё может сохранить копию или сделать снимок экрана. Но они позволяют не оставлять дверь открытой без причины.

Чек-лист: «Нужно ли сервису это знать?»

Перед регистрацией или выдачей разрешения остановитесь на минуту и ответьте на пять вопросов.

1. Какова цель сбора? Понятно ли, какую функцию поддерживают эти данные? Если сервис просит контакты, потому что предлагает «найти друзей», но вы не собираетесь пользоваться поиском, цель не делает разрешение обязательным для вас.

2. Поле действительно обязательно? Проверьте, помечено ли оно как обязательное, и попробуйте пройти даль-

ше без него. Иногда звёздочка означает техническое требование формы, а не необходимость для самой услуги.

3. К каким данным или функциям просят доступ?

Не смешивайте регистрацию с доступом к контактам, фотографиям, микрофону или геолокации. Это разные решения, и каждое заслуживает отдельного ответа.

4. Как долго будут храниться данные и можно ли их удалить? Указан ли срок, есть ли настройки удаления аккаунта, можно ли отключить синхронизацию? Если ответ неясен, не обязательно немедленно уходить, но стоит оценить ценность сервиса и чувствительность сведений.

5. Что произойдёт, если я откажусь? Перестанет работать вся услуга или только дополнительная функция? «Без этого удобнее» не означает «без этого невозможно».

Добавьте к ним шестой вопрос: **какую пользу получаю именно я?** Если обмен неравноценен — например, за небольшой купон просят доступ к адресной книге, — можно отказаться от бонуса. Иногда лучшая настройка приватности — не заполненная форма.

Вернёмся к Марине. Дата рождения была нужна для бонуса, но не для покупки. Контакты — только для поиска знакомых. Геолокация помогала показывать магазины поблизости, но их адреса можно было посмотреть вручную. Вход через соцсеть сокращал число нажатий, зато давал сервису доступ к данным профиля. Марина могла пользоваться приложением и без большей части этих разрешений. Она не обяза-

на была считать запросы подозрительными; достаточно было отличить обязательное от необязательного.

Как применить это к устройствам и семье

Проведите короткую ревизию разрешений на телефоне. Откройте настройки конфиденциальности и последовательно посмотрите, какие приложения имеют доступ к геолокации, контактам, фотографиям, микрофону и камере. Не нужно лишать всех всего: навигационному приложению местоположение необходимо, а видеозвонку — камера и микрофон. Вопрос в том, совпадает ли разрешение с функцией и нужно ли оно постоянно.

Затем проверьте общие устройства. У каждого взрослого пользователя по возможности должна быть собственная учётная запись. На семейном компьютере гостевой профиль пригодится посетителю; детская учётная запись позволяет настроить возрастные ограничения, не открывая ребёнку родительские покупки и документы. Это не замена разговору о безопасности, но хорошая граница между разными уровнями доступа.

В семейных сервисах и умном доме полезно заранее определить роли. Не каждому жильцу нужен доступ к настройкам камер, платежам или управлению аккаунтом владельца. Приглашайте членов семьи отдельными профилями, если сервис это поддерживает, и выдавайте права по их задачам. Общая учётная запись кажется простой, пока кто-нибудь случайно не удалит данные, не изменит настройки или

не унесёт пароль вместе со старым телефоном.

Разделение удобно лишь тогда, когда им можно пользоваться каждый день. Если система требует запоминать, какой из двенадцати адресов применён к конкретному сайту, она не выдержит бытовой нагрузки. Выберите несколько ясных категорий, подпишите их и не создавайте сложную конструкцию, которую невозможно поддерживать. Хорошая защита — та, что приживается.

Если лишний доступ уже выдан

Отзыв разрешения не отменяет прошлого. Приложение могло уже скопировать данные, а человек, получивший ссылку, — сохранить файл. Но отзыв всё равно важен: он ограничивает дальнейший доступ.

Действуйте по порядку:

1. Найдите источник доступа. Проверьте настройки телефона и раздел безопасности самого сервиса. Разрешение приложению и подключение стороннего аккаунта могут управляться в разных местах.

2. Отзовите ненужные права. Отключите геолокацию, контакты, фотографии или доступ подключённого приложения, если вы больше не пользуетесь функцией.

3. Проверьте, что осталось. Убедитесь, что приложение продолжает работать в нужном режиме. Посмотрите, можно ли удалить импортированные контакты, сохранённые данные или аккаунт целиком.

4. Закройте лишние копии и ссылки. Уберите доступ

к общим папкам, смените настройки ссылки, при необходимости задайте новый срок действия.

5. Если есть признаки чужого входа, действуйте шире. Завершите активные сеансы и защитите основной аккаунт. Подробно поговорим об этом в следующей главе.

Вероятно, часть функций после отзыва станет недоступна. Это не означает, что решение было неправильным: вы просто выбрали удобство осознанно. Если обнаружится, что доступ всё-таки необходим, его можно вернуть.

Небольшой план с большим эффектом

Не нужно за один вечер перестраивать всю цифровую жизнь. Выберите три изменения, которые легко поддерживать:

- при следующей регистрации оставьте необязательные поля пустыми и не связывайте аккаунты автоматически;
- отключите у одного приложения разрешение, которое не соответствует его основной функции;
- отделите покупки и рассылки от важной личной или рабочей переписки;
- создайте отдельный профиль для гостя на общем устройстве;
- замените общий доступ к папке на доступ только к нужному файлу.

Для упражнения выберите один часто используемый сервис и выпишите, что он знает о вас, к чему имеет доступ и какие функции вы реально используете. Напротив каждого

пункта поставьте одно из трёх решений: «нужно», «полезно, но необязательно» или «не использую». Затем измените хотя бы одну настройку из последней категории. Маленькое действие превращает абстрактное намерение в контроль.

Минимизация уменьшает количество сведений, которые могут попасть под удар. Разделение не позволяет одной проблеме автоматически открыть все сферы жизни. Наименьшие привилегии сужают круг того, что может сделать приложение, устройство или другой пользователь. Вместе эти принципы не создают непроницаемую стену — они делают последствия вероятной ошибки меньше и управляемее. А когда лишние связи и разрешения убраны, следующий шаг становится яснее: надёжно защитить те аккаунты, которые вы решили сохранить.

Аккаунты под защитой: уникальные пароли, менеджеры паролей и многофакторная аутентификация

В 7:12 утра Марине пришло уведомление: «Вход в аккаунт с нового устройства». Она не входила. Пока телефон лежал на кухонном столе, кто-то уже пытался попасть в её почту, интернет-магазин и социальную сеть. В двух местах попытки удались.

Марина не была беспечной. Она просто пользовалась паролем, который придумала много лет назад: имя кота, год его появления и восклицательный знак. Со временем пароль оброс цифрами, но не изменился по сути. Он открывал почту, магазин, форум, которым Марина давно не пользовалась, и ещё несколько сервисов. Когда один из них пережил утечку базы, пароль оказался в чужих руках. Осталось проверить, где он подходит ещё.

Это не история о гениальном взломщике, который месяцами охотился именно за Мариной. Чаще всё устроено прозаичнее: украденные или опубликованные пары «адрес электронной почты — пароль» автоматически проверяют на других популярных сайтах. Если пароль повторяется, одна утеч-

ка превращается в универсальный ключ. А если он ещё и предсказуем, менять в нём одну цифру на другую почти бессмысленно.

Хорошая новость в том, что защиту можно выстроить без сверхспособностей и без необходимости помнить десятки сложных комбинаций. Достаточно изменить подход: у каждого аккаунта — свой пароль, хранит их менеджер, а самые важные входы требуют дополнительного подтверждения.

Как один пароль становится цепочкой

Пароль — это не просто секретная фраза. Это ключ от конкретной двери. Но когда один и тот же ключ подходит к почте, магазину и банковскому сервису, любая утечка превращает его в связку ключей от всего дома.

Повторное использование паролей опасно даже тогда, когда каждый отдельный сервис кажется неважным. Старый форум может быть заброшен, но его пароль способен открыть аккаунт, которым вы пользуетесь каждый день. А почтовый ящик часто служит мастер-ключом: через него можно сбрасывать пароли, получать ссылки для восстановления и подтверждать смену настроек. Захват почты нередко означает возможность постепенно перехватить и другие учётные записи.

Именно поэтому Марина обнаружила проблему не там, где ожидала. Сначала в магазине появилась незнакомая попытка входа. Затем пришло письмо о смене пароля в соцсети. Она немедленно проверила почту — и увидела в спис-

ке активных сеансов неизвестное устройство. Не произошло ничего похожего на киношную сцену: не погас свет, не заговорил зловещий голос. Но чужой человек мог читать письма, искать в них чеки и ссылки для восстановления, а затем пробовать следующие двери.

Если вы получили неожиданное уведомление о входе, не нажимайте на ссылку в письме или сообщении, пока не убедились, что оно настоящее. Откройте приложение или введите адрес сервиса самостоятельно. Проверьте входы и устройства, завершите незнакомые сеансы, смените пароль на уникальный и включите дополнительную защиту. Если доступ к почте уже потерян, действуйте через официальную процедуру восстановления сервиса; при риске для платежей свяжитесь с банком или платёжной организацией по проверенному номеру. Не отвечайте на сообщения, которые предлагают «срочно вернуть аккаунт» за деньги или просят назвать код подтверждения.

Главное — не ругать себя за прежнюю привычку. Люди не проектировались для запоминания десятков случайных строк. Когда память перегружена, мы упрощаем задачу: повторяем пароль, меняем одну цифру, добавляем восклицательный знак. Это понятный человеческий компромисс — и именно его стоит поручить инструменту.

Длина и уникальность важнее хитрых замен

Пароль вроде K0t!2017 выглядит сложным: заглавная буква, цифра вместо буквы, знак препинания. Но человеку лег-

ко догадаться, как он устроен, а автоматической проверке — испытать распространённые шаблоны и варианты. Замена «о» на «0» не превращает знакомое слово в крепость.

Для повседневной защиты полезнее два правила:

1. Пароль должен быть уникальным. Если он утечёт с одного сайта, он не откроет другие аккаунты.

2. Пароль должен быть достаточно длинным и случайным. Чем больше возможных вариантов, тем сложнее подобрать его перебором.

Именно менеджер паролей позволяет соблюсти оба правила, не превращая жизнь в экзамен по запоминанию. Человек запоминает одну длинную мастер-фразу, а приложение создаёт и хранит отдельные непредсказуемые пароли для каждого сайта. На практике это надёжнее, чем пытаться придумать для каждого сервиса «сложный», но похожий пароль.

Не нужно придумывать хитрую формулу вроде «название сайта плюс любимая цифра». Если правило известно или его можно угадать, разные пароли оказываются родственниками. Менеджер должен генерировать их независимо. Для важных аккаунтов выбирайте длинные случайные сочетания, а для сервисов, которые не позволяют вставить пароль, используйте достаточно длинную парольную фразу, если сервис это поддерживает.

Менять пароль просто по календарю обычно не требуется, если нет признаков компрометации и сервис не требует этого по обоснованным причинам. Частая обязательная смена

может лишь подтолкнуть к предсказуемым вариантам вроде «Пароль1», «Пароль2». Но если пароль повторялся, попал в утечку, был введён на подозрительной странице или вы получили уведомление о неизвестном входе — его нужно заменить сразу, причём на уникальный.

Менеджер паролей: связка ключей, которую тоже надо беречь

Менеджер — это защищённое хранилище для паролей, заметок и иногда кодов восстановления. Он может быть отдельным приложением, встроенным в операционную систему или браузер. Важно не то, насколько эффектно он выглядит, а насколько удобно и безопасно им пользоваться каждый день.

При выборе обратите внимание на несколько вещей:

- Поддерживает ли менеджер ваши устройства и браузеры, чтобы пароли было удобно сохранять и подставлять.
- Есть ли шифрование хранилища и понятное объяснение, кто и при каких условиях может получить к нему доступ.
- Можно ли включить многофакторную аутентификацию для самого менеджера.
- Есть ли безопасная синхронизация между устройствами и понятный способ сделать резервную копию.
- Можно ли экспортировать данные, если вы решите перейти на другой продукт.

Не выбирайте менеджер только по громкому названию,

но и не скачивайте неизвестное приложение из случайной рекламы. Проверьте официального разработчика, политику безопасности и инструкции по восстановлению. Встроенное хранилище может быть вполне подходящим решением, если оно доступно на ваших устройствах и вы умеете им пользоваться. Наилучший менеджер — не абстрактно самый совершенный, а тот, которым вы действительно будете пользоваться постоянно.

В центре хранилища — **мастер-пароль**. Он открывает остальные пароли, поэтому его нельзя повторять на других сайтах. Сделайте его длинным и таким, чтобы вы могли надёжно запомнить: например, сочетанием нескольких случайно выбранных слов. Не берите цитату, строчку песни или фразу, которую легко связать с вами. Если менеджер предлагает многофакторную защиту, включите её.

Запишите мастер-пароль только на время освоения, если боитесь забыть, и храните запись в безопасном физическом месте, а не на заметном листке возле компьютера. Не отправляйте его себе по почте и не храните в незашифрованном файле рядом с хранилищем. Уточните заранее, что произойдёт, если вы забудете мастер-пароль: у некоторых менеджеров восстановление невозможно именно потому, что разработчик не может прочитать ваши записи. Это не обязательно недостаток, но важное условие, которое нельзя узнавать в момент беды.

При первом запуске не нужно переносить в менеджер всё

цифровое прошлое за один вечер. Начните с главной почты и финансовых аккаунтов. Затем добавляйте пароли по мере входа в другие сервисы. Когда менеджер предложит заменить повторяющиеся или слабые пароли, меняйте их по одному и проверяйте, что новый вход действительно работает.

Если менеджер предупреждает, что пароль встречался в утечке, воспринимайте это как повод для замены именно на этом сервисе. Не вводите пароли в сторонние сайты «для проверки надёжности». И не сохраняйте мастер-пароль в браузере или другом хранилище, которое открывается тем же самым ключом: смысл защиты — не класть единственный ключ в незапертую коробку рядом с дверью.

Дополнительный фактор: ещё одна проверка, не ещё один пароль

Даже уникальный пароль может быть украден. Его можно выманить поддельной страницей входа, перехватить на заражённом устройстве или получить из новой утечки. Поэтому у важных аккаунтов стоит включить **многофакторную аутентификацию**, или MFA: подтверждение входа не только паролем, но и другим способом.

Факторы обычно делятся на три группы: то, что вы знаете (пароль), то, чем владеете (телефон или аппаратный ключ), и то, чем вы являетесь (например, биометрический признак). На практике многое зависит от сервиса: он может предлагать не все варианты, а биометрия на устройстве часто лишь разрешает доступ к сохранённому ключу, а не отправляет отпе-

чаток пальца сайту.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.