Техника цифровой безопасности

2026

Содержание

Прежде чем начать

Начинайте с темы «Пароли»: она закрывает больше реального риска, чем многие другие действия вместе.

В гайде девять основных тем по 10–15 минут и бонусная десятая тема «Основы работы с нейросетями»; в каждой есть конкретное действие, которое можно выполнить сразу. Темы идут от самой полезной к менее полезной, поэтому остановиться можно в любой момент: всё прочитанное до этого уже работает.

Пароли и менеджер паролей

Один и тот же пароль на тридцати сайтах — это не расхлябанность, а совершенно нормальный способ жить, когда регистрации просят отовсюду: от кофейни с бонусами до налоговой. Слабое место ровно одно: рано или поздно какой-нибудь из этих тридцати сайтов сольёт базу, и тот же пароль автоматически попробуют на почте, в банке и на маркетплейсе.

Сделай это прямо сейчас

- ☐ Скачать KeePassXC с keepassxc.org — 3 минуты
- ☐ Создать базу и придумать мастер-пароль — 7 минут
- ☐ Сменить пароль на почте и сохранить новый в базу — 5 минут
- ☐ Удалить старый пароль из последней переписки — 3 минуты
- ☐ Перенести в базу ещё один старый сайт, который вспомнится первым — 5 минут

Один пароль везде — это не лень, это одна дырка на тридцать замков

Дело не в том, что ваш пароль от почты слабый. База, которая утечёт, скорее всего принадлежит какому-нибудь форуму про рыбалку, о существовании которого вы забыли ещё в две тысячи каком-то году. Но пароль там записан тот же самый, что и на почте, — а дальше это уже не ваша проблема с памятью, а чужой сценарий: связку логин-пароль прогоняют по спискам популяр-

ных сервисов автоматом, без участия человека, пока где-нибудь не сработает. Ключи от квартиры и кредитки вы же не раскладываете по подъезду — а один и тот же пароль на тридцати сайтах устроен ровно так же.

Менеджер паролей: запомнить один, остальные — не ваша забота

Решение звучит подозрительно просто: запоминать надо один пароль, а не тридцать. Остальные хранит программа — менеджер паролей, база, запертая на этот единственный пароль. Возьмём KeePassXC: он открытый и бесплатный, а главное — база лежит обычным зашифрованным файлом `.kdbx`, который можно хранить локально или в надёжном облаке.

Установка

1. Откройте официальный сайт keepassxc.org и нажмите `Download` / `Скачать`.
2. Выберите свою операционную систему и скачайте официальный установщик с сайта KeePassXC.
3. Запустите установщик, нажимайте `Next` / `Далее`, затем `Install` / `Установить` и в конце `Finish` / `Готово`.
4. Откройте KeePassXC. Результат: программа запускается, но базы пока нет.

Создание базы

1. Нажмите `Create new database` / `Создать новую базу данных`.
2. Введите понятное имя базы, например `Пароли`; при желании добавьте короткое описание. Нажмите `Continue` / `Продолжить`; имя будущего файла будет с расширением `.kdbx`. (☒ создание базы).
3. KeePassXC показывает шаг защиты новой базы `Encryption Settings` / `Параметры шифрования`. В простом режиме

настройте только Decryption Time / Время расшифровки; рекомендация этой инструкции — около 3 секунд, но это не обязательное требование KeePassXC. Подберите время, которое остаётся приемлемым на самом медленном вашем устройстве. Нажмите Continue / Продолжить.

4. Оставьте формат KDBX 4, завершите ввод мастер-пароля на следующем экране и нажмите Done / Готово. Затем сохраните файл с расширением .kdbx в выбранном надёжном месте, нажав Save / Сохранить.

KeePassXC — настольная программа для Windows, macOS и Linux. Официального мобильного приложения KeePassXC нет: на Android и iOS используют совместимые сторонние клиенты, поэтому их интерфейс может отличаться.

Видео: Видео о KeePassXC: установка, база, генератор и синхронизация https://www.youtube.com/watch?v=CRM93f377Q4

Видео о KeePassXC: установка, база, генератор и синхронизация — подсказка к этому сценарию; названия элементов интерфейса могут отличаться от текущей версии.

- 15 с — установка
- 1:05 — создание базы
- 2:26 — генератор
- 4:55 — синхронизация

Иллюстрация: Encryption Settings / Параметры шифрования, включая Decryption Time / Время расшифровки.

Заводим базу и мастер-пароль

Выберите один вариант. Цель у обоих одна: получить мастер-пароль длиной больше 20 символов и не менее 100 bit по оценке KeePassXC. Отдельные правила безопасного хранения и проверки базы действуют независимо от выбранной дорожки.

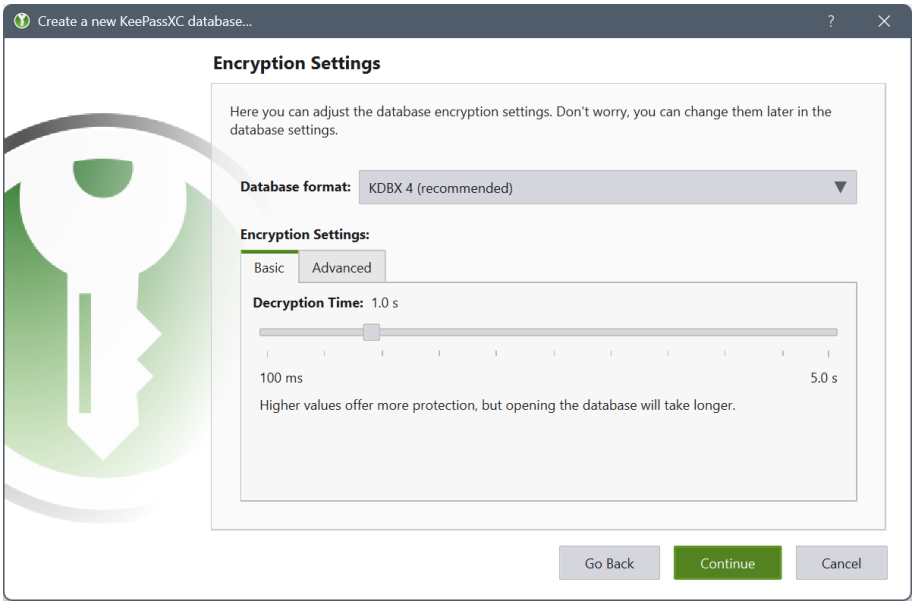

Рис. 1: Экран Encryption Settings / Параметры шифрования KeePassXC: Decryption Time / Время расшифровки

Придумаю мастер-пароль сам

Придумайте новую запоминаемую passphrase из нескольких слов, которые раньше не встречались вместе, и наберите её при включённой английской раскладке. Добавьте цифры и 1–2 спецсимвола, например `!"#;%:?*()`. Не используйте фразу из книги, песни, известного текста или популярную цитату, имя, дату рождения, другие личные данные или текст из соцсетей. Не превращайте известную фразу в пароль простой заменой букв и не используйте мастер-пароль повторно на других сайтах.

Ориентир — больше 20 символов и не менее `100 bit` по оценке KeePassXC.

Вот безопасный учебный пример преобразования, а не пароль для использования:

```
АлексейНеТакойУжДинозавр
-> FktrctqHtNfrjqE;Lbyjpfdh
-> #FktrctqHtNfrjqE;Lbyjpfdh^
-> 11#FktrctqHtNfrjqE;Lbyjpfdh^28
```

1. `АлексейНеТакойУжДинозавр` — исходная фраза из нескольких слов, записанная слитно для примера.
2. `-> FktrctqHtNfrjqE;Lbyjpfdh` — фраза набрана английскими буквами по выбранному правилу замены: регистр сохраняется, а сами буквы меняются.
3. `-> #FktrctqHtNfrjqE;Lbyjpfdh^` — в начало и конец добавлены специальные символы # и ^.
4. `-> 11#FktrctqHtNfrjqE;Lbyjpfdh^28` — в начало и конец добавлены цифры, чтобы увеличить длину и разнообразие символов.

Это только демонстрация механики, а не способ сделать известную фразу безопасной: простая транслитерация и замена букв не защищают предсказуемую фразу от подбора. Для реального мастер-пароля используйте новую уникальную passphrase из слов, которые раньше не встречались вместе, или криптографический генератор.

Это публичный учебный пример. Не копируйте его и не используй-

те как свой мастер-пароль.

Сгенерирую мастер-пароль в программе

Откройте встроенный Генератор паролей рядом с полем или через Инструменты -> Генератор паролей в KeePassXC. Выберите режим passphrase или пароля, задайте длину больше 20 символов и доступный состав: включите цифры и 1–2 спецсимвола. Проверьте оценку силы и примите только результат не менее `100 bit`; (☒ генератор). Не выбирайте результат, похожий на цитату или известный текст.

Убедитесь, что сможете ввести выбранный секрет. Правила его хранения описаны в общем блоке ниже. Не используйте учебный пример выше как мастер-пароль.

Видео: Дополнительная подсказка о надёжном мастер-пароле https://www.youtube.com/watch?v=pAUzloZkxWE

Дополнительная подсказка о надёжном мастер-пароле — общий ролик о выборе надёжного пароля; без привязки к конкретному моменту.

Общие действия после выбора

Введите выбранный пароль и повторите его в окне `Database Credentials` / `Учётные данные базы`. До запоминания храните секрет только на бумаге, отдельно от файла `.kdbx`, в защищённом месте; не используйте заметки, скриншоты, облако или устройство рядом с базой. После запоминания запись уничтожьте либо оставьте как отдельный аварийный офлайн-резерв с контролем доступа.

В простом режиме экран `Encryption Settings` / `Параметры шифрования` настраивает время расшифровки. В простой форме меняйте только это время; остальные параметры KDF и шифрования без понимания последствий не меняйте.

Иллюстрация: Database Credentials / Учётные данные базы, где мастер-пароль вводят и подтверждают.

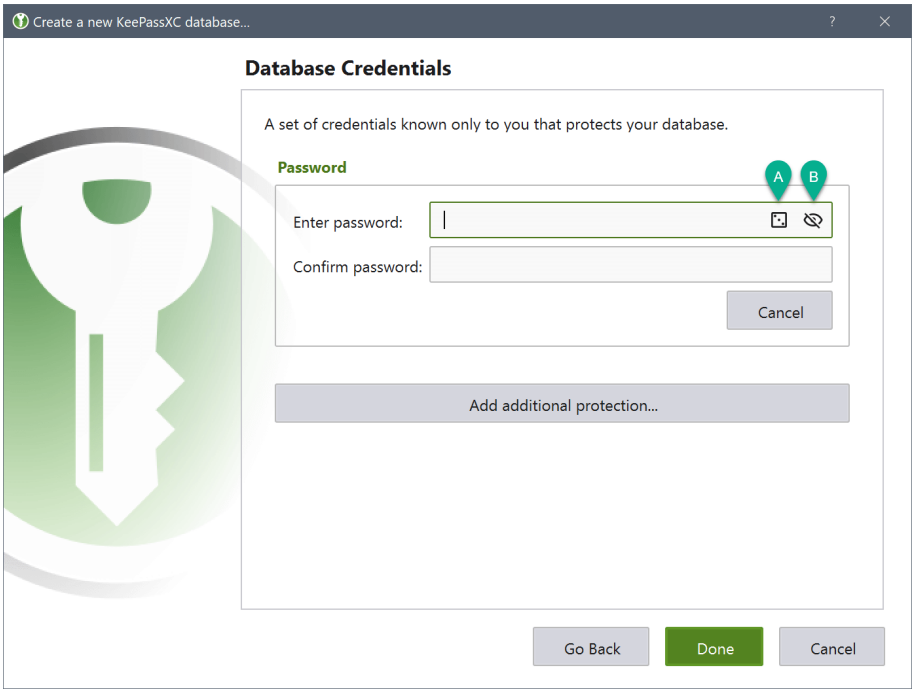

Рис. 2: Окно Database Credentials / Учётные данные базы KeePassXC

В ту же базу мастер-пароль положить нельзя: до базы он нужен для открытия. После подтверждения закройте базу через `Database` / `База данных` -> `Lock Database` / `Заблокировать базу данных`, затем снова откройте её и введите мастер-пароль. Результат: база открывается только с выбранным секретом.

> **Максимум**
>
> Выберите одну дорожку. В обоих случаях нужны длина больше 20 символов, не менее `100 bit` по оценке KeePassXC и безопасное хранение секрета отдельно от базы.

> **Максимум**
>
> Файл-ключ не включайте без заранее проверенного плана резервного копирования. Если он нужен, откройте `Database` / `База данных` -> `Database Settings` / `Параметры базы данных` -> `Security` / `Безопасность` -> `Add Key File` / `Добавить файл-ключ` -> `Generate` / `Создать`, сохраните файл отдельно от `.kdbx`, сделайте отдельную копию и проверьте открытие с мастер-паролем и key file. Для recovery-набора при восстановлении соответствующая копия `.kdbx` и matching key file должны быть доступны вместе, но храниться в защищённых местах; мастер-пароль храните отдельно. Проверьте восстановление именно из этих копий. Потеря или изменение key file означает потерю доступа, даже если мастер-пароль известен. Не редактируйте и не изменяйте содержимое key file; сделайте защищённую резервную копию.

> **Максимум**
>
> Время расшифровки увеличивает стоимость каждой проверки мастер-пароля и каждой офлайн-попытки взлома украденного файла. Слишком большое значение замедлит открытие

базы, поэтому проверьте его на самом медленном устройстве, которым реально будете открывать базу. Рекомендация этой инструкции — около 3 секунд, но это редакционный ориентир, а не требование KeePassXC. Проверка замедляется примерно пропорционально выбранному времени, поэтому измерьте результат на своих устройствах вместо того, чтобы полагаться на фиксированную оценку. Время расшифровки не заменяет длину пароля: биты — сколько вариантов перебирать, время — сколько стоит одна попытка; они перемножаются, и медленная база с коротким паролем не спасёт. Эта настройка живёт в самом файле базы, а не в программе, поэтому на более медленном устройстве та же база может открываться дольше, чем на ноутбуке, где вы её настраивали. Если это устройство слишком медленное для комфортного открытия, уменьшите значение, но не ниже выбранного минимума.

- ☐ При создании новой базы настроить время расшифровки в мастере защиты до завершения создания базы; KDF в расширенных настройках не менять.

Максимум

KeePassXC поддерживает аппаратную challenge-response защиту с YubiKey и OnlyKey. Это отдельная продвинутая функция, а не обычная 2FA и не TOTP. Перед включением изучите её ограничения и порядок восстановления в официальном руководстве KeePassXC.

Проверь себя. Что нужно сделать при создании базы?

1. Выбрать одну дорожку, получить секрет длиной больше 20 символов и проверить оценку не ниже `100 bit`.
2. Ввести и подтвердить выбранный мастер-пароль в `Database Credentials` / `Учётные данные базы`.
3. Положить мастер-пароль в новую запись той же базы.

Второй. После выбора одной из дорожек введите и подтвердите

мастер-пароль в учётных данных базы. Секрет храните отдельно от базы; оценка силы не является гарантией.

Получилось — когда файл базы создан, а мастер-пароль от него вы набираете по памяти или достаёте из безопасного отдельного места.

Генератор: остальные пароли — не ваша забота вообще

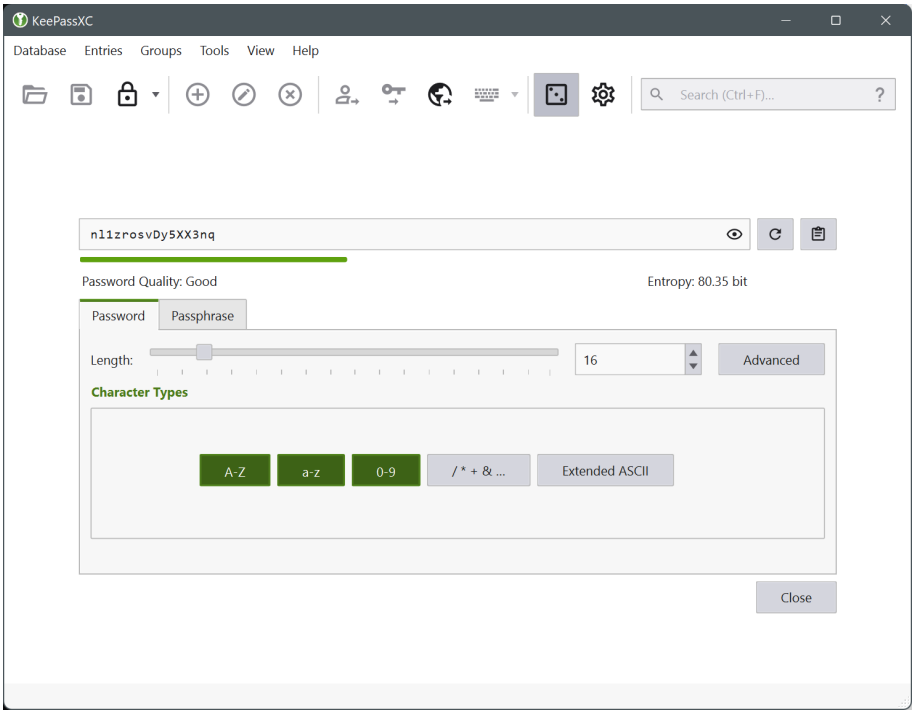

Рис. 3: Окно Password Generator / Генератор паролей KeePassXC для создания пароля записи

Иллюстрация: Password Generator / Генератор паролей для обычного пароля записи; тот же встроенный генератор может создавать случайную passphrase для мастер-пароля.

Для каждой обычной записи не придумывайте пароль вручную:

1. Нажмите Add Entry / Добавить запись.
2. Заполните поля Title / Название, Username / Имя пользователя и Password / Пароль.
3. Откройте Password Generator / Генератор паролей рядом с полем пароля или через Tools / Инструменты -> Password Generator / Генератор паролей.
4. Сгенерируйте пароль и проверьте оценку не ниже 100 bit, лучше 128 bit.
5. Нажмите Apply / Применить или Use Password / Использовать пароль, чтобы применить сгенерированный пароль в запись.
6. При необходимости заполните Notes / Заметки, нажмите OK / OK, чтобы закрыть редактор записи, затем Save / Сохранить, чтобы сохранить базу.
7. Скопируйте пароль через Copy Password / Копировать пароль, вставьте его в форму официального сайта и затем нажмите Clear Clipboard / Очистить буфер обмена.
8. Результат: в базе сохранена запись с логином и тем же сгенерированным паролем, который был передан сайту.

Расширение для браузера: настроили разок — дальше пароль подставляется сам

Сама программа пароль никуда не вставляет — подставлять логин и пароль прямо в форму на сайте умеет расширение для браузера. Без него база работает как справочник: пароль всё равно приходится копировать руками и вставлять в поле. С расширением она подставляет его сама, за один клик на странице входа.

Ниже — сразу расширение под ваш браузер; если не угадали, жмите «Показать все варианты» и выбирайте сами.

- KeePassXC Browser — Chrome Web Store — обычная установка одной кнопкой.
- KeePassXC Browser — Firefox Add-ons — то же самое для Firefox.

- KeePassXC Browser — Microsoft Edge Add-ons — отдельный магазин Edge, ставится так же просто.
- KeePassXC Browser — тот же Chrome Web Store — у Brave нет своего магазина, он ставит расширения Chrome напрямую.
- KeePassXC Browser — тот же Chrome Web Store — Yandex Browser тоже на Chromium, но сначала включите в настройках расширений «разрешить установку расширений из других каталогов».
- Документация KeePassXC по установке в Safari — поддержка Safari пока «предварительная» (с версии 1.10.0, март 2026), отдельного листинга в App Store ещё нет; актуальный порядок установки смотрите в документации, а надёжный запасной вариант на Safari уже сегодня — встроенный в KeePassXC Auto-Type.

Расширение вы уже поставили — осталось один раз связать его с самой базой, и дальше подстановка пароля будет работать сама. Прежде чем начинать, откройте KeePassXC и разблокируйте базу мастер-паролем: без открытой базы ни один из шагов 1–4 не сработает.

1. В KeePassXC откройте `Application Settings` / `Настройки приложения` — через шестерёнку в панели инструментов или через меню приложения, точный путь немного отличается в зависимости от ОС и версии.
2. Перейдите на вкладку `Browser Integration` / `Интеграция с браузерами`, включите `Enable browser integration` / `Включить интеграцию с браузерами` и отметьте галочкой тот браузер, для которого вы поставили расширение в предыдущем шаге (в списке он показан под своим обычным названием — Google Chrome, Firefox и так далее, без перевода).

Иллюстрация: вкладка Browser Integration / Интеграция с браузерами — чекбокс Enable browser integration / Включить интеграцию с браузерами и список браузеров с отметками.

3. В браузере откройте иконку KeePassXC-Browser на панели расширений (если её не видно, закрепите её через меню расширений — значок «кусочек пазла») и нажмите `Connect`. Про-

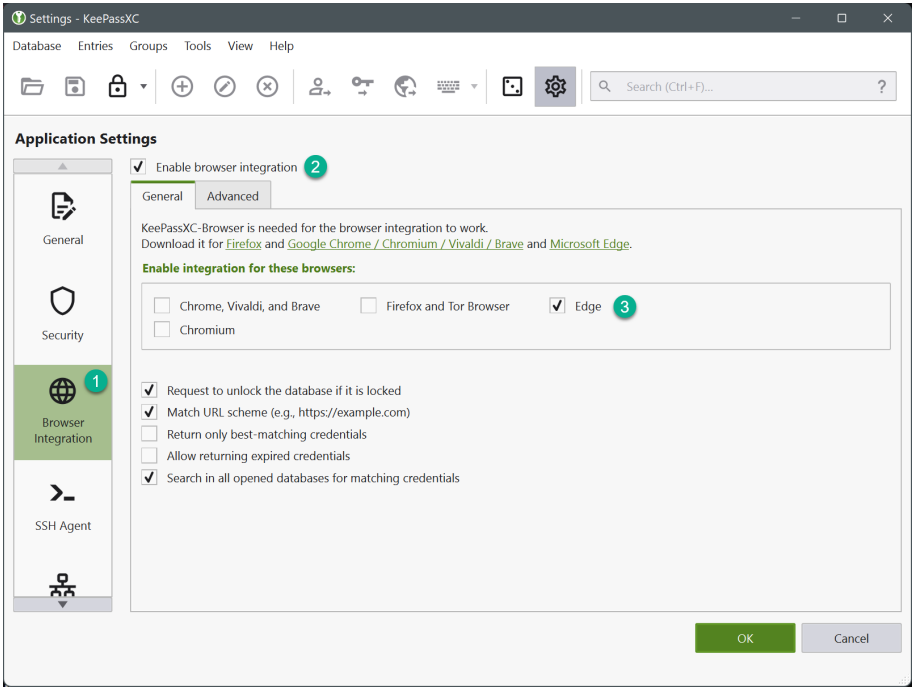

Рис. 4: Окно Application Settings / Настройки приложения KeePassXC: вкладка Browser Integration / Интеграция с браузерами

верить русский перевод этой кнопки не удалось: очень часто она остаётся англоязычной даже при русской локали браузера, так что не удивляйтесь.

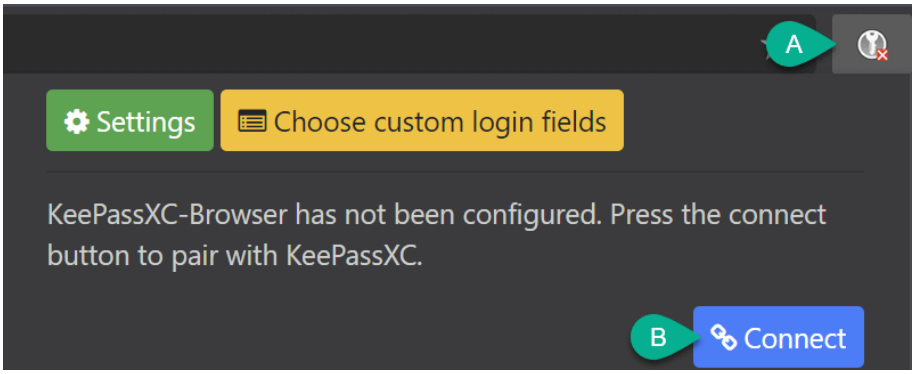

Рис. 5: Всплывающее окно расширения KeePassXC-Browser до подключения к KeePassXC

Иллюстрация: всплывающее окно расширения до подключения — кнопка Connect запускает связку с KeePassXC.

4. В окне KeePassXC появится диалог `KeePassXC - New key association request` / `KeePassXC - Запрос на ассоциацию нового ключа`. Впишите любое понятное название — например, имя браузера или устройства — и нажмите `Save and allow access` / `Сохранить и разрешить доступ`.

Иллюстрация: New key association request / Запрос на ассоциацию нового ключа — поле с названием связки и кнопка Save and allow access / Сохранить и разрешить доступ.

Если расширение стоит в нескольких браузерах, повторите шаги 3–4 в каждом — связка работает отдельно для каждого. И учтите: связали один раз — не значит работает вечно без программы. Чтобы автозаполнение сработало прямо сейчас, KeePassXC должен быть запущен, а база — разблокирована.

Получилось — когда иконка расширения в панели браузера показывает подключённое состояние, а на сайте с сохранённой в базе записью оно само предлагает подставить логин и пароль в форму

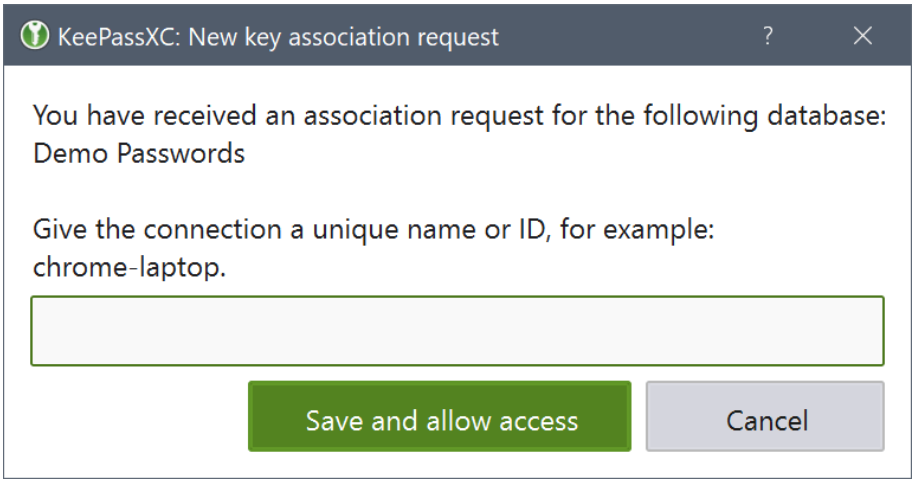

Рис. 6: Диалог New key association request / Запрос на ассоциацию нового ключа KeePassXC

входа.

С чего начать переезд

Начинайте с почты: через неё восстанавливается доступ ко всему остальному, так что это и есть единая точка отказа — и её стоит забрать у памяти в первую очередь. Дальше — по своему усмотрению и в своём темпе. Десять сайтов из тридцати, переведённых на менеджер, — уже победа сама по себе, а не промежуточный результат по пути к полному переходу. Полный переход не обязателен вовсе: остальные двадцать подождут сколько угодно, никуда не денутся.

На практике это значит:

1. Откройте настройки почты, найдите смену пароля — обычно в разделе «Безопасность» или «Пароль и вход».
2. В KeePassXC откройте существующую запись через `Edit Entry` / `Изменить запись`.
3. Откройте `Password Generator` / `Генератор паролей`, сгенерируйте новый пароль и проверьте оценку не ниже `100 bit`, лучше `128 bit`.

4. Нажмите Apply / Применить / Use Password / Использовать пароль, чтобы сгенерированный пароль попал в запись.
5. Введите новый пароль на официальном сайте почты и завершите смену пароля.
6. В редакторе записи нажмите OK / OK, чтобы закрыть его, затем Save / Сохранить, чтобы сохранить базу: первая кнопка закрывает редактор записи, вторая записывает изменения в файл базы.
7. Выйдите из почты и войдите снова с логином и паролем из сохранённой записи.
8. Нажмите Clear Clipboard / Очистить буфер обмена и заблокируйте базу.

Если записи нет, сначала используйте полный сценарий обычной записи: Add Entry / Добавить запись, Title / Название, Username / Имя пользователя, Password / Пароль.

Получилось — когда пароль от почты сменён, а в базе рядом с логином лежит новый сгенерированный пароль, а не старый по памяти.

Куда деть базу и как её не потерять

Рабочая база должна иметь несколько проверенных копий в разных надёжных местах: на другом носителе и, при необходимости, у доверенного облачного провайдера. Зашифрованный файл .kdbx можно хранить в облаке, но мастер-пароль, key file и экспорт не должны лежать рядом с базой в незашифрованном виде. Выбирайте носитель или провайдера с историей версий и автоматическими резервными копиями, храните отдельные проверенные копии и периодически тестируйте восстановление. Мастер-пароль храните отдельно от базы в защищённом месте.

Проверяйте резервные копии восстановлением, а не только наличием файлов.

Копия на другом устройстве должна быть именно отдельной проверенной копией, а не единственным синхронизированным двойником. Мастер-пароль храните отдельно от базы в защищённом месте.

Максимум

Синхронизировать `.kdbx` между телефоном и ноутбуком можно через доверенное облако: оно видит зашифрованный файл. Сначала сделайте отдельную резервную копию, затем дождитесь окончания синхронизации, откройте базу на втором устройстве и проверьте несколько групп и записей. CSV/XML можно использовать для разовой миграции, но не оставляйте незашифрованный экспорт. После миграции удалите временные файлы и очистите корзину; для постоянного хранения используйте `.kdbx`. Изменения на двух устройствах одновременно могут конфликтовать, поэтому перед редактированием убедитесь, какой файл актуален.

- ☐ Положить копию базы на второе устройство и убедиться, что она там открывается.

Финальная проверка

1. Закройте KeePassXC и снова откройте `.kdbx`: база должна запросить мастер-пароль, а при включённом key file — и его.
2. Откройте обычную запись и проверьте, что `Title` / `Название`, `Username` / `Имя пользователя` и `Password` / `Пароль` сохранены; пароль не должен быть в чате или заметках браузера.
3. Заблокируйте базу через `Lock Database` / `Заблокировать базу данных`, выберите `Clear Clipboard` / `Очистить буфер обмена` и убедитесь, что копия `.kdbx` лежит отдельно от рабочего файла.
4. Результат: база открывается, запись актуальна, буфер очищен, а резервная копия существует и не является единственным файлом.

Ещё один сайт — и так, пока не останется забытых

Почта уже переехала — самая опасная дыра закрыта. Остальное можно закрывать не отдельным вечером, а по одному сайту за раз,

каждый раз, когда об этом сайте всё равно вспомнили: заходите на него, меняете пароль на сгенерированный и сохраняете запись в базу тем же способом, что уже отработали на почте.

1. Вспомните любой сайт, где до сих пор стоит старый пароль по памяти.
2. Смените его пароль на сгенерированный так же, как для почты: генератор, сохранение в базу, выход и вход с новым паролем.
3. Повторите для следующего сайта, когда снова о нём вспомните — без графика и без единого дедлайна на весь список.

Получилось — когда для этого конкретного сайта в базе тоже лежит свежий пароль. А когда таких сайтов в жизни почти не осталось — тот самый забытый форум про рыбалку можно смело списать в отставку и не считать долгом: десять переехавших сайтов из тридцати уже были победой, а не промежуточным результатом.

Удалить старый пароль из последней переписки

Новый пароль защищает почту только с момента смены. Если старый пароль когда-то отправлялся в SMS, письме или обычном чате, он всё ещё лежит в истории и может попасться тому, кто получит доступ к переписке.

Откройте последнюю переписку, где вы отправляли пароль, удалите сообщение у себя и у собеседника, если сервис это позволяет, а затем смените пароль ещё раз, если уже не уверены, где он успел засветиться.

Получилось — когда старого пароля нет в последней переписке, а при сомнении он заменён новым.

Как передать пароль другому человеку — один раз, а не навсегда

Иногда пароль всё-таки приходится кому-то передать: пароль от Wi-Fi пришедшему мастеру, доступ к сервису — родственнику.

Дать соседке ключ, чтобы полить цветы, пока вы в отпуске, — нормально. Оставить тот же ключ в почтовом ящике на два года просто потому, что так однажды было удобно, — уже нет. Сообщение с паролем и есть тот самый почтовый ящик: SMS, обычная переписка в мессенджере и письмо никуда не деваются сами — они лежат в истории, уезжают в облачную копию переписки и достаются каждому, кто потом войдёт в этот аккаунт или просто возьмёт телефон в руки. Дело не в мастере и не в родственнике, оба тут ни при чём, — дело в том, что переписка живёт куда дольше, чем повод, ради которого пароль был отправлен.

Самый простой вариант — сказать пароль вслух или передать его при личной встрече: не нужно создавать ссылку или оставлять сообщение. Если это невозможно — почта, разные города, мастер, к которому неудобно подходить каждый раз, — не отправляйте пароль текстом напрямую, а воспользуйтесь одним из способов ниже: они показывают пароль получателю один раз и потом сами его удаляют. Ни один способ не даёт абсолютной тайны: получатель всё ещё может сфотографировать экран, пересказать пароль или сохранить его другим способом.

- **Секретные чаты Telegram:** в профиле получателя выберите «Начать секретный чат» и отправьте пароль сообщением с таймером самоуничтожения. Переписка шифруется из конца в конец, не сохраняется в облаке Telegram и не пересылается — Telegram блокирует пересылку сообщений из секретных чатов. Это отдельная опция: включать её нужно каждый раз заново и на каждом устройстве, обычные чаты Telegram сами в секретные не превращаются.

Специальные сайты для одноразовой передачи. Это другой подход: не функция внутри мессенджера, а отдельный сервис, который создаёт одну ссылку, показывает секрет один раз и сам её убивает.

- **Bitwarden Send (самый надёжный вариант здесь):** используйте официальную документацию Bitwarden Send, задайте короткий срок жизни и, если доступно для выбранной настройки, максимум одно открытие или удаление после открытия. Можно добавить отдельный пароль; получателю

не обязательно иметь аккаунт Bitwarden. Данные шифруются на вашей стороне ещё до отправки — сервер получает уже зашифрованный текст и никогда не видит пароль, а Bitwarden как компания регулярно публикует независимые аудиты безопасности — список отчётов. Остальные сервисы из этого списка тоже с открытым кодом и решают ту же задачу — у Bitwarden просто более развёрнутая и регулярно проверяемая независимыми аудиторами история.

- **Onetime Secret:** создайте одноразовую ссылку на onetimesecret.com. Сервис описывает удаление секрета после первого открытия.
- **Password Pusher:** создайте ссылку на pwpush.com с одним открытием и коротким сроком действия, если эти параметры доступны при создании ссылки.
- **PrivateBin:** создайте самоуничтожающуюся заметку на privatebin.net — публичном инстансе открытого проекта PrivateBin с шифрованием на стороне браузера (AES-256-GCM: сервер получает уже зашифрованные данные). Задайте срок жизни и, если нужно, режим «сгорает после прочтения» перед отправкой.
- **Yopass:** создайте секрет на yopass.se — публичной демоверсии открытого проекта Yopass с шифрованием OpenPGP на стороне браузера ещё до отправки на сервер, одноразовым просмотром и сроком жизни от часов до недель. Для по-настоящему чувствительных данных сам проект советует разворачивать Yopass у себя, а не полагаться на публичный демо-сервер.

После разовой передачи смените пароль: он больше не должен оставаться действующим после того, как необходимость закончилась.

> **Максимум**
>
> Secret Chats в Telegram — отдельная функция поверх обычного мессенджера. Signal и Session построены вокруг приватности с самого начала, а не добавляют её отдельной кнопкой поверх обычной переписки — это следующий шаг, если готовы поставить отдельное приложение.

- **Signal:** отправьте пароль исчезающим сообщением с коротким таймером через официальную настройку Signal. Получатель всё равно может сделать скриншот, поэтому таймер не заменяет доверие.
- **Session:** Session не требует номера телефона или почты — переписка привязана к случайному Account ID, а не к вашей личности. Включите исчезающие сообщения с коротким сроком хранения. Как и в Signal, это только сокращает срок хранения в интерфейсе и не мешает получателю сделать скриншот, сфотографировать экран или скопировать пароль.

Максимум

Там, где доступ нужен нескольким людям на постоянной основе — стриминг, семейный тариф, — отдавать свой личный пароль не лучший вариант, даже самым надёжным способом. У сервиса почти всегда есть штатный механизм: добавить человека в семейный план или завести ему отдельный профиль. Это лучше передачи собственного логина хотя бы потому, что доступ выдаётся и забирается отдельно от вашего: закрыть его одному человеку можно, не меняя пароль себе и не трогая остальных.

Максимум

Бывает и обратный случай: доступ и правда должен быть общим — пароль администратора домашнего роутера, семейный сейф с близким человеком. Тут не «поделиться своим паролем», а завести с самого начала общую базу: у KeePassXC есть встроенное слияние баз, так что каждый вносит свою правку на своём устройстве, а потом их сводят в одну, не затирая чужие изменения.

☐ Завести общую базу KeePassXC с близким человеком для

паролей, которые нужны вам обоим, — например для администратора домашнего роутера.

Проверь себя. Пришёл мастер чинить стиральную машину и просит пароль от Wi-Fi. Какие способы передать его оставят пароль лежать в истории надолго? Отметьте всё, что подходит.

1. Отправить в SMS.
2. Написать обычным сообщением в мессенджере.
3. Отправить письмом на почту.
4. Сказать вслух.
5. Отправить исчезающим сообщением, которое сотрётся через минуту.

Первые три. Дело не в мастере — дело в том, что сообщение переживёт этот визит на годы: оно уедет в облачную копию переписки, останется в истории и достанется каждому, кто потом войдёт в этот аккаунт или просто возьмёт телефон в руки. Сказать вслух — бесплатно и надёжнее всего. Исчезающее сообщение — компромисс для случая, когда вслух никак. А пароль от гостевой сети после такого визита стоит поменять: разовая надобность закончилась, а пароль остался.

Управлять своими логинами и паролями — базовый навык в цифровом мире, вот прямо как умение не терять ключи от квартиры. В следующей теме — про двухфакторную аутентификацию: вторую линию обороны, которая срабатывает даже тогда, когда пароль всё-таки утёк.

Двухфакторная аутентификация

Пароль от почты может утечь не потому, что вы сделали что-то не так, а потому что где-то далеко слили базу чужого сервиса — и дальше тот же пароль на автомате прогонят по всем крупным сайтам: вдруг сработает и у вас. Пароль тут работает как код на домофоне: подсмотреть, подобрать, узнать у знакомого соседа — дело нехитрое, а вот в квартиру с ним всё равно не попадёшь, пока на двери есть замок под ключ. Второй фактор и есть тот самый ключ: пароль у посторонних уже есть, а войти всё равно не получается.

Сделай это прямо сейчас

- ☐ Поставить на телефон приложение-генератор кодов — 3 минуты
- ☐ Включить второй фактор на почте — 6 минут
- ☐ Включить «Облачный пароль» в Telegram — 4 минуты
- ☐ Включить двухшаговую проверку в WhatsApp — 3 минуты
- ☐ Сохранить резервные коды от почты в базу паролей — 3 минуты

Приложение-генератор на телефоне

Приложение-генератор показывает шестизначный код и меняет его каждые тридцать секунд (в настройках сервисов такой код подписан словом TOTP). Считает его сам телефон — интернет для этого не нужен вовсе.

Android: Aegis Authenticator, из Google Play или F-Droid

1. Поставьте Aegis — бесплатный и открытый: из Google Play или из F-Droid, если Play на телефоне не работает. Приложение одно и то же.
2. Откройте его. При первом запуске Aegis попросит выбрать, чем запирать хранилище: пароль, а если телефон умеет — ещё и разблокировку по отпечатку. Берите оба: отпечаток на каждый день, пароль как запасной вход.
3. Пароль придумайте новый и сразу сохраните в KeePassXC: `Add Entry` / `Добавить запись` -> `Title` / `Название` (например, `Aegis — хранилище`) -> `Password` / `Пароль` -> `OK` / `OK` при закрытии редактора -> `Save` / `Сохранить`. После этого нажмите `Clear Clipboard` / `Очистить буфер обмена` и `Lock Database` / `Заблокировать базу`. Забудется — хранилище не открыть ни здесь, ни на новом телефоне.
4. Внутри будет пустой список. Так и надо: первая запись появится на следующем шаге, вместе с почтой.

Официально: getaegis.app.

iPhone: Ente Auth, из App Store

1. Поставьте Ente Auth из App Store — тоже бесплатное и открытое.
2. Откройте его. Аккаунт создавать не обязательно: на стартовом экране можно выбрать работу без резервной копии — тогда приложение целиком живёт в телефоне и обходится без интернета.
3. Резервную копию в облаке (зашифрованную, уже с аккаунтом) можно включить когда угодно потом, из настроек. На то, как считаются коды, это не влияет.
4. Список будет пустой. Так и надо: первая запись появится на следующем шаге, вместе с почтой.

Если Ente не приглянулся, из открытых и бесплатных есть ещё 2FAS — он тоже работает без регистрации.

Официально: ente.com/auth.

Если у сервиса варианта с приложением нет вовсе — включайте смс

и не думайте: номер иногда удаётся увести на чужую сим-карту, но даже такой второй замок несравнимо лучше, чем его отсутствие.

Получилось — когда приложение стоит на телефоне и открывается, а внутри пусто. Так и должно быть: первый код появится на следующем шаге, когда вы добавите туда почту.

Максимум

Есть вариант понадёжнее приложения — аппаратный ключ: физическая флешка размером с обычный USB-накопитель (YubiKey — самый узнаваемый пример), которую подключают к порту или подносят к телефону по NFC и один раз касаются пальцем. От фишинга он защищает не потому, что код сложнее подделать, а потому что ключ вообще не выдаёт код: он сам проверяет адрес сайта, на который вы заходите, и на поддельном домене просто отказывается срабатывать — даже если вы сами не заметили подмену в адресной строке. Стоит такой ключ обычно от двух-трёх тысяч рублей и выше, и для большинства аккаунтов это уже не первый шаг, а следующий — после того как приложение-генератор уже стоит и работает.

- ☐ Посмотреть в настройках безопасности почты, поддерживает ли она аппаратный ключ.

Почта: главный вход

Начинать стоит с почты: через неё восстанавливается доступ почти ко всему остальному. Кто попал в почту, тот закажет восстановление пароля куда угодно — и никакой другой замок уже не важен.

Почта: Gmail и Google-аккаунт, с компьютера

1. Откройте myaccount.google.com — в том же Chrome, где уже открыта почта; заново входить не придётся.
2. В меню слева — раздел «Безопасность и вход» (в части версий он подписан короче, просто «Безопасность»).
3. В блоке «Вход в Google» нажмите «Включить двухэтапную

аутентификацию».

4. Дальше Google ведёт сам: подтвердить пароль и выбрать способ. Обычно он сразу предлагает уведомление на ваш Android-телефон или смс-код — любого из них уже достаточно, второй фактор с этого момента включён.
5. Приложение-генератор кодов, которое вы поставили на прошлом шаге, добавляется там же, в перечне способов входа внутри «Двухэтапной аутентификации». Смс при этом никуда не денется сама — но коды можно будет брать из приложения, а её оставить запасным вариантом.
6. Вернитесь в тот же раздел «Двухэтапная аутентификация», найдите строку «Резервные коды», а в ней — «Получить резервные коды». Их десять, каждый восьмизначный и срабатывает ровно один раз. Вкладку не закрывайте: коды понадобятся на последнем шаге чек-листа.

Официально: как включить двухэтапную аутентификацию и про резервные коды.

В любой другой почте настройка живёт примерно там же — в разделе «Безопасность» (Security) настроек аккаунта. Иногда она прячется на вкладку глубже, во «Вход и восстановление» или «Конфиденциальность», но почти всегда её находит поиск по настройкам по слову «безопасность».

Получилось — когда в настройках напротив двухэтапной аутентификации значится «Включена», а при следующем входе с нового устройства почта спрашивает не только пароль.

Telegram: «Облачный пароль»

У Telegram второй фактор устроен не так, как везде: это не одноразовый код из приложения, а обычный дополнительный пароль, который мессенджер спросит при входе с нового устройства — вдобавок к смс-коду. Поэтому в русском интерфейсе он и называется «Облачным паролем»: искать его в настройках стоит по слову «пароль», а не «фактор». Мессенджер идёт сразу после почты: там завязаны переписка и контакты. (☒ настройка облачного пароля). Правила выбора канала и запрет на отправку секретов разобраны

в разделе «Защищённая и незащищённая связь».

Telegram на Android: «Облачный пароль»

1. Откройте Telegram, дальше — Settings / Настройки.
2. Раздел Privacy and Security / Конфиденциальность и безопасность (в некоторых версиях название или расположение может отличаться).
3. Пункт «Облачный пароль». В английском интерфейсе — Two-Step Verification.
4. Придумайте пароль и повторите его. Новый, не тот же, что от почты, — и сразу сохраните в KeePassXC по короткому сценарию записи: Add Entry / Добавить запись, Title / Название, Password / Пароль, OK / OK, затем Save / Сохранить, Clear Clipboard / Очистить буфер обмена и Lock Database / Заблокировать базу.
5. Подсказку к паролю можно пропустить. А вот резервную почту укажите: если облачный пароль забудется, вернуть доступ поможет именно она.
6. На эту почту придёт код подтверждения — введите его, и всё.

Официально: FAQ Telegram про 2-Step Verification — страница только на английском, русской версии у неё нет.

Видео: Tech Talk — How to Secure Telegram | Complete Guide https://www.youtube.com/watch?v=_TjEEv-Inro

Tech Talk — How to Secure Telegram | Complete Guide — подсказка именно к Telegram и его «Облачному паролю», не к Aegis или TOTP.

- 46 с — облачный пароль и 2FA
- 2:49 — активные сеансы
- 5:01 — история захвата аккаунта

Активные сеансы проверяйте в том же разделе настроек; (☒ где открыть список сеансов).

Получилось — когда в настройках напротив «Облачного пароля» значится, что он включён, а на резервную почту пришло подтверждение.

WhatsApp: двухшаговая проверка

В WhatsApp это отдельный PIN, который защищает перенос аккаунта на новый телефон. Он не заменяет код из SMS, а добавляет к нему ещё один секрет, который мошеннику придётся узнать отдельно.

WhatsApp на Android и iPhone: двухшаговая проверка

1. Откройте WhatsApp ⊠ «Настройки» ⊠ «Аккаунт» ⊠ «Двухшаговая проверка».
2. Нажмите «Включить», придумайте новый шестизначный PIN и повторите его.
3. Добавьте почту для восстановления, если WhatsApp её предложит, и сохраните PIN в KeePassXC по короткому сценарию записи: `Add Entry` / `Добавить запись`, `Title` / `Название`, `Password` / `Пароль`, `OK` / `OK`, затем `Save` / `Сохранить`, `Clear Clipboard` / `Очистить буфер обмена` и `Lock Database` / `Заблокировать базу`. Не храните PIN рядом с паролем от самого аккаунта.

Получилось — когда в разделе «Двухшаговая проверка» написано, что она включена.

Резервные коды: на случай утопленного телефона

При включении второго фактора сервис показывает резервные коды — десяток одноразовых кодов на случай, если телефон потерялся, разрядился или утонул в раковине. Показывает обычно один раз, прямо при настройке: у части сервисов коды можно перевыпустить и позже, но только пока вход в аккаунт ещё работает — если доступ уже потерян, перевыпускать будет нечем. Поэтому кладите их туда же, где лежат пароли, — в базу KeePassXC из темы про пароли, отдельной записью.

Резервные коды: отдельная запись в KeePassXC

1. На экране сервиса откройте раздел резервных кодов: на-

пример, в Google это «Двухэтапная аутентификация» -> «Резервные коды» -> «Получить резервные коды». Не закрывайте экран, пока запись не проверена.

2. Откройте базу KeePassXC и нажмите New Group / Новая группа (или фактическое название этой команды в вашей версии), задайте имя группы Двухфакторная аутентификация / Two-factor authentication.
3. В этой группе нажмите Add Entry / Добавить запись и создайте отдельную запись, не смешивая её с записью пароля аккаунта.
4. Заполните поля: Title / Название: Google — резервные коды — личная почта; Username / Имя пользователя: email аккаунта; Password / Пароль: оставить пустым, потому что кодов несколько; Notes / Заметки: каждый код на отдельной строке, ровно как показал сервис, без склеивания и без лишней нумерации.
5. Нажмите Save / Сохранить, перепроверьте число и содержимое кодов с экраном сервиса и только после этого закройте экран сервиса.
6. При использовании кода нажмите Clear Clipboard / Очистить буфер обмена, а после завершения работы нажмите Lock Database / Заблокировать базу.
7. Результат: коды находятся в отдельной группе и записи, а не в названии, чате или скриншоте. Пустое поле Password здесь относится только к набору резервных кодов, а не ко всем записям KeePassXC.

Используйте один код за раз: скопируйте его, вставьте в форму входа и после этого выберите Clear Clipboard / Очистить буфер обмена. После успешного входа удалите только использованный код из Notes / Заметки, нажмите Save / Сохранить и заблокируйте базу через Lock Database / Заблокировать базу данных». Не удаляйте остальные коды.

Резервные коды не заменяют TOTP: TOTP — это короткий код из приложения- генератора, а резервный код используется один раз, когда генератор недоступен. Получив резервные коды заново, откройте существующую запись, замените старый набор в Notes / Заметки, нажмите OK / OK при закрытии редактора, затем Save /

Сохранить. Снова сверьте с сервисом число и содержимое кодов, удалите копию из буфера через Clear Clipboard / Очистить буфер обмена и заблокируйте базу через Lock Database / Заблокировать базу.

Получилось — когда запись сохранена, лишние копии кодов закрыты, использованный код удалён, а база заблокирована.

KeePassXC: отдельная база для TOTP

KeePassXC умеет хранить секрет TOTP и показывать одноразовые коды. Но чтобы сохранить смысл двух факторов, создайте для них отдельную базу, например two-factor-tokens.kdbx. Не кладите TOTP в тот же .kdbx, где лежат пароли. Основную базу паролей и TOTP-базу храните раздельно, по возможности на разных защищённых носителях или хотя бы в разных местах. Это не превращает один секрет в два независимых фактора: TOTP-секрет всё равно остаётся чувствительным и тот, кто его получил, сможет генерировать коды.

KeePassXC 2.7.x: добавить TOTP в отдельную базу

1. Откройте отдельную базу two-factor-tokens.kdbx в KeePassXC. Создайте или выберите запись нужного сервиса.
2. Откройте контекстное меню TOTP / TOTP -> Set up TOTP... / Настроить TOTP....
3. В поле Secret Key / Секретный ключ вставьте только Base32-секрет. Не вставляйте целиком otpauth:// URI.
4. Оставьте Default settings (RFC 6238) / Настройки по умолчанию (RFC 6238), если сервис не сообщил другие параметры. При нестандартных настройках проверьте Algorithm / Алгоритм, Time step / Шаг времени и Code size / Размер кода по инструкции сервиса.
5. Нажмите OK / OK, затем Save / Сохранить.
6. Для входа откройте контекстное меню записи -> Show TOTP / Показать TOTP или скопируйте TOTP. После вставки кода в форму входа очистите буфер обмена.

Системные часы компьютера и телефона должны быть точными:

TOTP зависит от времени, и даже небольшой сдвиг может сделать код недействительным.

Aegis: перенос без прямого импорта

Прямого импорта хранилища Aegis в KeePassXC нет. Перенос делают через экспорт, а затем вручную переносят секрет конкретной записи.

Aegis: перенести одну запись в KeePassXC

1. В Aegis откройте `Settings` / `Настройки` -> `Import & Export` / `Импорт и экспорт` -> `Export` / `Экспорт`.
2. Выберите зашифрованный экспорт `Aegis (.JSON)` / `Aegis (.JSON)` или другой формат, который предлагает установленная версия приложения. Если Aegis показывает `Encrypt the vault` / `Зашифровать хранилище`, включите шифрование и задайте новый пароль экспорта.
3. Передайте файл только защищённым способом и откройте его локально. Найдите нужную запись и извлеките из её `otpauth://` URI только Base32-значение после `secret=`. QR-код и весь URI в KeePassXC не переносите и нигде не публикуйте.
4. В отдельной TOTP-базе KeePassXC настройте запись по шагам выше, вставив только это значение `secret=`.
5. Если понадобится восстановить Aegis, используйте `Settings` / `Настройки` -> `Import & Export` / `Импорт и экспорт` -> `Import from file` / `Импортировать из файла`.

Перед удалением чего-либо сравните текущий код KeePassXC и Aegis в одном временном окне и выполните вход в сервис. Только после успешной проверки удаляйте временный экспорт, корзину и временные копии.

> **Максимум**

Инварианты безопасности

- TOTP-база KeePassXC хранится в отдельном файле, не рядом и не на том же устройстве или носителе, где находится основная парольная база.
- Резервный экспорт Aegis хранится в отдельном зашифрованном файле и в отдельном месте: не в публичном чате, обычной почте, незашифрованной папке или рядом с `.kdbx`.
- Не удаляйте единственную рабочую копию до проверки импорта, совпадения кода и успешного входа в сервис.
- Экспорт TOTP-секретов по чувствительности равен ключу для генерации кодов. Доступ к нему компрометирует TOTP. Если одна и та же запись остаётся и в Aegis, и в KeePassXC, это две копии одного секрета, а не два независимых фактора.
- Для постоянного резервирования держите минимум две зашифрованные копии в разных местах. Это отдельное требование к резервированию, а не замена требованию хранить основную TOTP-базу отдельно от парольной.

Вся цена второго фактора — пять лишних секунд на новом устройстве или после переустановки браузера: открыть приложение, подсмотреть код, ввести; на своём телефоне не будет и этого, пока сессия жива.

Если сводить тему к одной мысли: это тот самый ключ, который не разбросаешь по подъезду вместе с паролем, — и стоит он ровно те пять секунд, за которые чужая утечка пароля перестаёт быть вашей проблемой. В следующей теме — про обновления: самая скучная и самая недооценённая привычка, которая закрывает дыры, о существовании которых вы могли вообще не знать.

Обновления ОС и приложений

«Напомнить позже» — возможно, самая нажимаемая кнопка на планете, и дело тут не в лени: обновление вечно вылезает в самый неподходящий момент, посреди работы, фильма или звонка. Десять минут один раз — и дальше можно вообще не думать, а разница между «включено» и «выключено» огромная.

Сделай это прямо сейчас

- ☐ Включить автообновление на телефоне — 3 минуты
- ☐ Поставить обновление, которое телефон откладывает уже месяц — 2 минуты
- ☐ Включить автообновление на компьютере и в браузере — 5 минут

«Обновлю потом» — это и есть дыра

Заплатка не только чинит дыру — она же и объявляет всему миру, что дыра там была. Вместе с обновлением производитель почти всегда публикует открытый список исправлений: что именно исправлено и в каких версиях. С этого момента про уязвимость знают все — включая тех, кто пишет скрипты, которые ищут в интернете непропатченные устройства не по одному, а сразу пачками.

Получается парадокс: до выхода патча про дыру не знал почти никто, кроме её автора, а сразу после выхода — знает весь мир, и ваш телефон вдруг оказывается в списке тех самых непропатченных.

Это как если бы вам прислали новый замок взамен старого — того самого, к которому в интернете выложили подробную инструкцию по вскрытию, — а вы оставили его лежать в коробке под дверью на полгода. Кто читал инструкцию, всё ещё может ей воспользоваться.

Проверь себя. Производитель закрыл дыру в марте и написал об этом в открытом бюллетене. Вы жали «Напомнить позже» до сентября. Сколько месяцев дыра была открыта именно у вас — при том что весь мир знал о ней с марта?

Шесть. В этом и весь фокус: обновление — это одновременно и заплатка, и объявление о том, где была дырка. С марта по сентябрь ваше устройство стояло с открытой дверью, к которой опубликована инструкция. Хорошая новость в том, что закрывается это одной галочкой в настройках, и дальше происходит без вас.

Речь не про будущее, а про то, что уже случилось

Львиная доля реально эксплуатируемых уязвимостей закрыта производителем далеко не вчера — обычно месяцы назад. Разговор не о гипотетической дыре, которую однажды найдут и придётся срочно латать в будущем. Дыра уже найдена, уже описана в открытых источниках, и патч для неё уже готов и лежит рядом с кнопкой «Установить». Всё, что остаётся сделать, — перестать быть тем самым устройством из статистики, которое месяцы спустя после выхода патча всё ещё работает на старой версии.

Телефон: автообновление в двух местах

На телефоне обновления живут в двух разных местах, и включить нужно оба: обновление самих приложений и обновление системы телефона. Это два разных переключателя в двух разных меню, один без другого не работает.

Android: приложения и система

1. Приложения: откройте Google Play, нажмите на значок своего профиля в правом верхнем углу ⊠ `Settings` / `Настройки`

☒ Network preferences / Настройки подключения ☒ Auto-update apps / Автообновление приложений ☒ выберите «Через любую сеть» (или «Только через Wi-Fi», если жалко мобильный трафик).

2. Система: пункт и путь к нему у каждого производителя свои. На Pixel — Settings / Настройки > «Система» > «Обновление системы». У Samsung и Xiaomi название и место этого пункта пляшут от модели к модели и от версии прошивки — вместо того чтобы гадать путь, надёжнее сразу открыть поиск по настройкам и вбить туда «обновление системы» или «обновление ПО»: такая строка поиска есть в обеих прошивках и не промахивается мимо переименований. Тот же приём сработает и на других телефонах, если пункта с привычным названием не нашлось — меню у части моделей отличается только формулировкой.
3. Оба переключателя включаются один раз, но совсем без вашего участия обновление всё равно не проходит: систему телефон иногда просит подтвердить перезапуск для установки — это одно нажатие, а не ручной поиск патча.

iPhone: приложения и система

1. Приложения: Settings / Настройки > App Store ☒ включите «Обновления приложений».
2. Система: Settings / Настройки > «Основные» > «Обновление ПО» > «Автоматические обновления» — здесь два отдельных переключателя, и нужны оба: «Автоматически загружать» скачивает обновление заранее, «Автоматически устанавливать» ставит его в фоне. Включён только первый — обновление каждый раз будет скачано, но так и останется висеть неустановленным, пока не нажмёте сами.
3. У автоматической установки есть условия: телефон должен заряжаться и быть подключён к Wi-Fi. Не выполняется хотя бы одно — iPhone отложит установку до следующей подходящей ночи, а не встанет молча.

Получилось — когда в обоих меню (приложения и система) автообновление на телефоне включено. Совсем без вашего участия всё равно не бывает — иногда попросит подтвердить перезапуск или

дождётся ночи на зарядке и Wi-Fi, — но искать кнопку «Установить» самому больше не придётся.

Компьютер и браузер: автообновление без напоминаний

На компьютере всё зависит от системы. В Windows 11 обновления и так ставятся автоматически по умолчанию — включать обычно ничего не нужно, разве что заглянуть в «Центр обновления Windows» и проверить, что они не поставлены на паузу и не отложены на дальний срок.

С Windows 10 всё иначе: обычная бесплатная поддержка закончилась в октябре 2025 года, и без отдельной подписки обновления безопасности на такой машине больше не выходят вовсе.

Windows 10: бесплатная программа расширенных обновлений (ESU)

1. Убедитесь, что стоит версия 22H2 (Windows Update покажет её сама) и что вход — под учётной записью Microsoft, а не локальной: программа ESU работает только с ней.
2. Откройте `Settings` / `Параметры` > «Обновление и безопасность» > «Центр обновления Windows» — если компьютер подходит, там появится пункт «Зарегистрироваться сейчас» (Enroll now).
3. Выберите способ подключения: бесплатно, если включена синхронизация настроек через резервную копию Windows Backup; бесплатно за 1000 баллов Microsoft Rewards; либо разовый платёж около 30 долларов (или в местной валюте) за годовую лицензию — она сразу покрывает до десяти устройств на одном аккаунте Microsoft.
4. Готово: обновления безопасности продолжат приходить до 12 октября 2027 года. В Евросоюзе и ЕЭЗ Microsoft раздаёт этот же год обновлений всем желающим бесплатно, без условия про резервную копию.

Не подключились или компьютер под программу не подходит — это и есть тот самый случай, «устройство, которое перестали об-

новлять», разобранный в разделе «Когда устройство пора менять» чуть ниже: загляните туда.

В macOS автоматическая загрузка и установка включаются в `Settings` / `Настройки` ☒ «Основные» ☒ «Обновление ПО». Значок информации рядом с пунктом автоматических обновлений может выглядеть иначе или отсутствовать; ищите это действие через настройки автоматических обновлений и включите загрузку и установку.

Отдельно — про браузер. Само обновление в популярных браузерах почти всегда и так включено по умолчанию, специально искать переключатель не нужно — разве что в Firefox: там в `Settings` / `Настройки` > «Основные» > «Обновления Firefox» стоит явный переключатель «Автоматически устанавливать обновления», и его стоит один раз проверить. (☒ проверка обновления). У Chrome и Edge отдельного переключателя в настройках нет вовсе — они обновляются сами в фоне, а проверить версию и заодно подтолкнуть обновление можно, вставив в адресную строку `chrome://settings/help` (Chrome) или `edge://settings/help` (Edge): откроется страница «О браузере», которая сама же проверяет наличие обновлений.

Применяется новая версия не сразу ни в одном из трёх браузеров: она скачивается в фоне сама, но включается только после перезапуска. Браузер обычно сам подсказывает момент — в меню или у иконки профиля появляется кнопка вроде «Перезапустить, чтобы обновить». (☒ обновление всех программ). (☒ список программ и удаление лишнего). Нажимать стоит именно её, а не закрывать окно вручную: только через эту кнопку браузер гарантированно восстанавливает все открытые вкладки, так что ничего не потеряется.

Получилось — когда автообновление на компьютере стоит на автомате (в Windows 11 оно и так уже было), а в браузере не осталось забытой кнопки «Перезапустить, чтобы обновить».

Видео: Tech Talk — WinGet для Windows: Как установить и обновить ВСЕ программы одной командой https://www.youtube.com/watch?v=KIJ76bjBr0Q

Tech Talk — WinGet для Windows: Как установить и обновить ВСЕ

программы одной командой — подсказка только для Windows и шага с обновлением программ; к Android, iOS и macOS не относится.

- 5:49 — обновление
- 6:10 — обновить всё
- 6:31 — список, установка и удаление

Уведомление, которое ждёт третий месяц

Если на телефоне уже который месяц висит значок «Доступно обновление», самый простой момент его наконец поставить — сегодня вечером, когда телефон и так лежит на зарядке.

Поставить отложенное обновление

1. Зайдите в раздел обновлений (пути для Android и iPhone — двумя разделами выше) и нажмите «Загрузить и установить» или просто «Установить», если обновление уже скачано.
2. Подтвердите перезапуск, когда попросит система, и оставьте телефон заряжаться — дальше он справится сам.

Самая частая причина, по которой обновление годами висит недоустановленным, — не лень, а нехватка места: и iOS, и Android для установки нужно немного свободного места под временные файлы, и без него значок просто виснет молча, без внятной ошибки.

iPhone: освободить место перед обновлением

1. «Настройки > Основные > Хранилище iPhone» — вверху список того, что система сама советует убрать, обычно самое безобидное: старые чаты, неиспользуемые приложения.
2. Быстрее всего — «Настройки > App Store» ☒ включить «Выгружать неиспользуемые приложения»: сами приложения удалятся, а их данные останутся, и при следующем запуске всё скачается заново.

Android: освободить место перед обновлением

1. «Настройки > Хранилище» ☒ «Освободить место» — система сама предложит удалить резервно скопированные фото и временные файлы.

2. Или откройте приложение «Файлы» (Files by Google либо аналог от производителя) ☒ пункт «Очистка» в боковом меню: там отдельно старые скриншоты, дубликаты и давно не открытые файлы.

Получилось — когда значок «Доступно обновление» пропал, а телефон работает на последней версии.

Когда устройство пора менять

Бывает и так, что автообновление включать уже некому: производитель официально прекратил выпускать обновления для конкретной модели, и патчей для неё больше не будет вообще, сколько ни жди. В этом случае у устройства два пути — заменить его или перестать использовать для важного. Почту и банковские приложения стоит перенести на то, что ещё получает обновления, а старый телефон или ноутбук можно оставить для менее чувствительных задач: читать новости, слушать музыку, — там цена ошибки заметно ниже.

Для компьютера на Windows 10 без ESU (или вообще любого старого железа, до которого обновления уже не доходят) есть три рабочих пути, и они не взаимоисключающие:

Старый Windows-компьютер: три пути

1. Обновиться до Windows 11, если позволяет железо. Проверить это можно официальным приложением Microsoft PC Health Check — ссылка на скачивание aka.ms/GetPCHealthCheckApp, после установки нужно нажать «Проверить сейчас». Приложение не ставит Windows 11 само, а просто честно говорит, чего не хватает: обычно это процессор из официального списка совместимости или выключенные в BIOS TPM 2.0 и Secure Boot.
2. Поставить Linux Mint — бесплатно, с рабочим столом, который выглядит и ведёт себя похоже на привычный Windows. Требует привыкания: часть специфичного софта — отдельные банк-клиенты, некоторые игры — под Linux не работает вовсе или работает через костыли. Скачать:

linuxmint.com/download.php.

3. Поставить ChromeOS Flex — тоже бесплатно, от Google, превращает старый компьютер в подобие Chromebook: браузер и веб-сервисы летают, а вот обычные десктопные программы (Photoshop, большинство игр, специфичный рабочий софт) не запустятся вовсе — Flex рассчитан на тех, кому от компьютера нужны в основном браузер и почта. Работает не на любом железе — список поддерживаемых моделей на support.google.com/chromeosflex, страница проекта — chromeos.google/products/chromeos-flex.

Максимум

У большинства крупных производителей план обновлений для конкретной модели опубликован отдельной страницей на сайте — по годам, а не общими словами вроде «поддерживается долго». У Google это официальная справка про сроки поддержки Pixel: support.google.com/pixelphone/answer/4457705. У Samsung — официальная страница про обязательства по обновлениям безопасности по моделям: security.samsungmobile.com/workS
У Apple отдельной страницы со сроками нет, но актуальный список моделей, которые получают конкретную версию iOS, публикует сама Apple — например, support.apple.com/guide/iphone (ссылка меняется под каждую новую iOS — ищите такую же по названию актуальной версии). Смотреть этот срок нужно **до** покупки следующего телефона, а не после: разница между моделью, которой обещали обновления ещё на пять лет, и моделью, у которой из обещанных двух лет уже прошёл один, — это разница в годах реальной защиты, а не мелкий шрифт в характеристиках.

- [ ] Открыть официальную страницу поддержки своей модели телефона и проверить, до какого года ей обещаны обновления.

Максимум

Самая забытая железка в доме — это роутер. У основных производителей есть собственное приложение с пуш-уведомлением и автообновлением прошивки: у TP-Link это TP-Link Tether, у ASUS — ASUS Router, у Keenetic — приложение «Keenetic». Если у вашего роутера такое есть, им и стоит пользоваться — проще, чем лезть в веб-интерфейс.

Если приложения нет, прошивка обновляется вручную через веб-интерфейс роутера — а вот адрес там не всегда один и тот же: `192.168.1.1` — самый частый вариант, встречается и `192.168.0.1`, а у части производителей вместо цифр свой домен — например, у TP-Link это `tplinkwifi.net`. Какой из них ваш, обычно написано на наклейке снизу роутера или показано в приложении производителя. Открыв админку, ищите там же, где меняете настройки Wi-Fi, раздел «Обновление прошивки» или «Firmware Update», и ставите последнюю версию. Роутер, который выдал провайдер, а не куплен отдельно, иногда вовсе не даёт доступ к этим настройкам — тогда обновление прошивки на совести провайдера, и это стоит просто иметь в виду.

Заодно, раз уж зашли, стоит проверить пароль администратора: у части моделей он до сих пор заводской — то самое «admin/admin», которое легко угадать, — а у более новых уникальный пароль уже напечатан на наклейке снизу. Если пароль всё ещё заводской, самое время его сменить.

- ☐ Зайти в настройки роутера, проверить обновление прошивки и заодно сменить заводской пароль администратора.

Из всех тем бюллетеня это единственная, где правильный ответ буквально «сделать один раз и больше не думать»: не нужно каждый раз заново решать, ставить обновление или отложить его ещё на неделю — включили автообновление, и дальше оно происходит само. В следующей теме — про фишинг: там, в отличие от обнов-

лений, придётся каждый раз включать голову заново, потому что окончательно автоматизировать это не получится.

Фишинг, поддельные сайты и сертификаты

Фишинг — самая массовая атака из всего бюллетеня, и целится она вовсе не в технику: антивирус, обновлённая система и даже пароль из менеджера тут ни при чём, потому что дверь в этой схеме открывает сам человек. Работает это не на глупости, а на спешке: письмо подгадано под момент, когда решение принимается за три секунды, а не за три минуты вдумчивого чтения.

Сделай это прямо сейчас

- ☐ Положить банк и почту в закладки и заходить только оттуда — 3 минуты
- ☐ Записать в контакты телефон банка с обратной стороны карты — 2 минуты
- ☐ Найти в почте последнее письмо «подтвердите данные» и рассмотреть адрес отправителя — 5 минут

Приём один: вас торопят и дают ссылку

Универсального шаблона фишингового письма не существует, а общий приём один: вас торопят и сразу подсовывают ссылку, по которой удобно поторопиться. Дальше — вариации на одну тему. «Счёт заблокируют через час, если не подтвердить данные». «Аккаунт закроют, если не войти прямо сейчас». «Курьер не смог вручить посылку — подтвердите адрес по ссылке». «Подтвердите карту, иначе платёж не пройдёт». Повод разный, механика одна:

короткий испуг или азарт, три секунды на решение, а решение — это клик.

Приём цепляет даже тех, кто прекрасно знает про существование фишинга, — потому что письмо про доставку приходит именно в тот день, когда посылка и правда должна была прийти, а про блокировку счёта — ровно тогда, когда вы читаете почту одним глазом между встречами. Дело не в вашей внимательности, а в подгаданном моменте, и хорошая новость в том, что одна привычка ниже закрывает почти все варианты разом, чем бы ни пугало очередное письмо.

Та же схема работает и через QR-код — квишинг, тот же трюк с подменой адреса, только код на бумажке вместо ссылки в письме. Стикер с чужим QR-кодом заклеивают поверх настоящего — на парковочном автомате, платёжном терминале, в меню кафе, — и на вид не отличить. Второй вариант — тот же QR-код прямо внутри письма: ссылку спам-фильтр и антивирус проверяют, а картинку с кодом внутри неё — нет. Правило то же самое, что и со ссылкой: камера телефона показывает адрес в превью ещё до перехода — прочитайте его там, прежде чем нажать «Открыть», а для оплаты надёжнее набрать известный адрес вручную или открыть официальное приложение банка, чем довериться коду на случайной бумажке.

Сначала раскрыть ссылку, а потом её читать

Правило «читать домен справа налево» бесполезно, пока адреса не видно вовсе, — а в почтовом приложении вместо ссылки часто просто кнопка «Подтвердить» или «Войти», без единой буквы адреса рядом. Прежде чем читать, ссылку нужно раскрыть, и делается это по-разному на компьютере и на телефоне.

Компьютер: навести курсор или скопировать адрес

1. Наведите курсор на ссылку или кнопку, не нажимая, — настоящий адрес появится в левом нижнем углу окна браузера, в строке состояния.
2. Если строки не видно или хочется рассмотреть адрес внима-

тельнее — щёлкните по ссылке правой кнопкой: в контекстном меню найдётся пункт про копирование адреса ссылки — формулировка чуть отличается в разных браузерах, но по смыслу он один.
3. Вставьте скопированное в любой текстовый редактор или в адресную строку браузера — но не нажимайте Enter, это способ прочитать адрес, а не перейти по нему.

Телефон: зажать ссылку пальцем

1. Нажмите на ссылку или кнопку и удерживайте палец — через секунду-две на экране появится меню действий или превью, и в нём, как правило, виден полный адрес.
2. Прочитайте адрес тем же способом — справа налево. Не похож на ожидаемый — просто уберите палец, не выбирая ни один из пунктов, и никуда не переходите.
3. Тот же приём часто работает и с адресной строкой самого браузера: если в ней виден только короткий домен, коснитесь строки — она обычно переходит в редактирование, и в нём виден полный адрес целиком.

Тот же фокус работает и тогда, когда ссылка спрятана за красивой кнопкой в письме — в Gmail, Apple Mail и любом другом почтовом приложении: зажмите кнопку пальцем на телефоне или наведите на неё курсор на компьютере, и адрес раскроется точно так же.

Официально: как распознать фишинговое письмо, Google.

Адрес читается справа налево, а не слева

Самая рабочая проверка — не стиль письма и не логотип в шапке, а адрес, на который на самом деле ведёт ссылка. Правило простое: смотрите на ту часть, которая стоит вплотную перед первой одинарной косой чертой (`/`), и читайте её справа налево. Почти всегда первым попадётся домен верхнего уровня (`.ru`, `.com`), а сразу за ним — настоящее имя сайта; у части адресов зона состоит из двух сегментов (`.co.uk`, `.com.ru`, `.msk.ru`) — тогда настоящее имя сайта стоит на шаг левее, но сам принцип «читать справа налево» не меняется. Всё, что стоит ещё левее через точку, — поддомены,

и это уже декорация: её пишет тот же, кто владеет настоящим доменом, а написать он может что угодно, хоть слово «банк» три раза подряд.

Это тот же фокус, что и с обратным адресом на конверте: отправитель пишет на конверте что хочет, и красивое «Ваш Банк» в уголке ничего не гарантирует — важно, куда конверт реально уйдёт, а не что написано слева от марки. В адресе сайта роль этого уголка играет ровно то, что стоит перед настоящим доменом.

Отдельно — всё, что стоит до символа @ в адресе: браузер эту часть попросту выбрасывает и идёт по тому, что после неё. `vashbank.ru@nekto.io/vhod` откроет `nekto.io`, а `vashbank.ru` здесь — просто подпись перед собачкой, которую никто не проверяет.

Проверь себя. Банк называется `vashbank.ru`. Из письма ведут четыре ссылки. Какая из них действительно на сайт банка?

1. `vashbank.ru.secure-login.com/vhod`
2. `online.vashbank.ru/vhod`
3. `vashbank-ru.com/vhod`
4. `vashbank.ru@nekto.io/vhod`

Вторая. Смотреть надо на то, что стоит вплотную перед первой одинарной косой чертой, и читать справа налево. В первой настоящий домен — `secure-login.com`, а `vashbank.ru` там просто приписан слева, как имя на чужом конверте. В третьей дефис вместо точки: `vashbank-ru.com` — совершенно другая контора. В четвёртой всё, что стоит до @, браузер выбросит, и вы окажетесь на `nekto.io`. Во второй слева приписан `online`, но само имя банка стоит там, где надо, — последним.

Тот же приём работает не только со ссылкой в письме, но и с самим отправителем: у него есть красивое имя вроде «Служба поддержки банка», а настоящий адрес с реальным доменом прячется за этим именем — виден он, только если по имени отправителя кликнуть или навести на него курсор. Откройте в почте последнее письмо на тему вроде «подтвердите данные» — такое почти наверняка найдётся — раскройте настоящий адрес отправителя одним из способов ниже и прочитайте домен после @ тем же способом: справа налево, по сегментам через точку.

Gmail: раскрыть настоящий адрес отправителя

1. На компьютере откройте письмо и нажмите на маленькую стрелку вниз под именем отправителя — развернётся строка с настоящим адресом и пометками «mailed-by» и «signed-by»: доменами, которые письмо реально отправили и подписали.
2. В приложении на телефоне откройте письмо, нажмите «Подробнее» и затем «Сведения о безопасности» — там те же самые «mailed-by» и «signed-by».
3. Значок вопросительного знака рядом с именем отправителя — отдельный тревожный сигнал: это сам Gmail не смог подтвердить подлинность письма.

Официально: как проверить подлинность письма.

Почта на iPhone: раскрыть адрес отправителя

1. Откройте письмо и нажмите на имя отправителя в шапке — на экране появится его настоящий адрес.
2. Прочитайте адрес тем же способом, что и в ссылке, — справа налево.

Получилось — когда вы нашли такое письмо, раскрыли настоящий адрес отправителя и прочитали его домен тем же способом, что и адрес в ссылке.

Дефис вместо точки — уже другая контора

Есть более грубый трюк, чем декорация слева от домена: не спрятать домен целиком, а слегка исказить его так, чтобы взгляд скользнул мимо. Дефис вместо точки — `vashbank-ru.com` вместо `vash bank.ru` — для браузера это совершенно другая контора, зарегистрированная кем угодно и когда угодно; для уставшего взгляда в конце длинного дня это одна и та же надпись. Здесь по-прежнему работает то же самое правило «справа налево» из раздела выше: дефис и лишний сегмент в адресе — это ровно то, что оно и создано ловить, символ за символом.

Есть и вариант похитрее: одну из латинских букв в адресе заменяют не на похожую, а на графически идентичную — букву из другого

алфавита, которая на экране рисуется теми же самыми пикселями, что и нужная латинская, например кириллическую «а» вместо латинской a. Раньше это было неотличимо на глаз, но современные Chrome, Firefox и Safari именно такую подмену умеют ловить сами: если в одном сегменте адреса смешались буквы из разных алфавитов, браузер показывает не красивую подделку, а её техническое имя — нечитаемую строку вида xn--... — и подмена сразу бросается в глаза без всякого чтения. Не ловится этим ровно один случай — буквы из одного и того же алфавита, которые просто похожи по рисунку, вроде латинских rn вместо m: смешения алфавитов там нет, ловить браузеру нечего. От такой подмены по-прежнему защищает не чтение, а привычка заходить не по ссылке, а по своей закладке: закладка ведёт туда, куда вы её сохранили сами, а не туда, куда её нарисовал шрифт.

Замочек: конверт запечатан, а не проверен на честность

Замочек в адресной строке подтверждает две технические вещи: канал зашифрован, то есть никто по дороге не подслушает, что вы вводите, — и сертификат выдан именно на тот домен, который сейчас в адресной строке. Он не означает, что на другом конце сидит честный человек. (⊠ как проверить сертификат). Это разница между запечатанным конвертом и проверкой того, что внутри написана правда, — конверт можно запечатать одинаково аккуратно что от банка, что от кого угодно ещё. Поддельный сайт получает свой собственный, совершенно настоящий замочек за несколько минут и бесплатно, и это никак не связано с тем, кто и зачем сайт создал.

Перед вводом чувствительных данных проверьте, что адрес начинается с HTTPS и что домен официальный. Сам по себе значок замка этого не доказывает: он подтверждает шифрование соединения и владение указанным доменом, но не честность сайта.

> **Максимум**
>
> Замочек выдаёт удостоверяющий центр — организация, кото-

рая выпускает сертификаты и подписывает их своей подписью; эту подпись браузеры и устройства заранее внесли в список доверенных, поэтому проверяют её автоматически, без вашего участия. При выдаче обычного сертификата центр проверяет ровно одну вещь: что запрашивающий действительно управляет доменом, на который просит сертификат, — например, через специальный файл на сервере домена, который может туда положить только тот, кто этим сервером управляет. Кто регистрировал домен, зачем и что собирается на нём разместить, удостоверяющий центр не проверяет вообще: это не входит в его задачу и не входит в то, что подтверждает замочек. Отсюда и вывод: домен `vashbank-ru.com` пройдёт ту же самую проверку с тем же результатом, что и настоящий `vashbank.ru`, — обе стороны получат свой честный замочек, потому что для выдачи сертификата это две равноправные и никак не связанные друг с другом конторы. (☒ опасность корневого сертификата).

На телефоне эта проверка не так удобна: путь к сведениям о сертификате там не такой очевидный, как на компьютере, — поэтому саму проверку логичнее делать за компьютером, а на телефоне полагаться на привычку заходить по своей закладке.

Видео: Tech Talk — Все об SSL-сертификатах: чем опасен Российский корневой SSL-сертификат https://www.youtube.com/watch?v=EA9Y1rBaF-o

Tech Talk — Все об SSL-сертификатах: чем опасен Российский корневой SSL-сертификат — подсказка к сертификатам и замочку, а не полный курс по фишингу.

- 2:26 — сертификат
- 5:33 — удостоверяющие центры и цепочка доверия
- 11:25 — опасность корневого сертификата
- 12:13 — атака посредника

☐ Открыть сайт своего банка, нажать на замочек и посмотреть, кому и кем выдан сертификат.

Один путь закрывает почти всё

Одно правило снимает почти все варианты фишинга разом: в банк и почту заходим своим путём — через приложение или свою собственную закладку, набранную один раз вручную, — а не по ссылке из письма или сообщения, кем бы оно ни было подписано. Настоящий банк переживёт, что вы зашли не по его ссылке, а вошли сами; поддельный — не переживёт, потому что ему больше неоткуда взять ваш пароль.

Правило работает даже тогда, когда письмо настоящее: если оно и правда от банка, почти всегда то же самое действие можно найти и в приложении, и на сайте, куда вы зашли сами, без всякой ссылки.

Адрес для этой закладки берите не из поиска и не из письма, а с обратной стороны карты, из договора с банком или прямо из официального приложения — там он всегда настоящий. Дальше дело за минуту: наберите адрес банка и почты в строке браузера вручную, один раз, и сразу добавьте страницу в закладки (`Ctrl+D` в большинстве браузеров на Windows и Linux, `Cmd+D` — на Mac, или звёздочка в адресной строке). На телефоне то же самое делается через меню браузера: в Chrome на Android — значок «⋮» в адресной строке ⋮ пункт про добавление в закладки; в Safari на iPhone — значок «Поделиться» ⋮ пункт про добавление в закладки или на экран «Домой» (точная формулировка отличается в разных версиях). Дальше заходите туда именно так — каждый раз, без нового набора адреса и уж тем более без ссылки из письма.

Получилось — когда банк и почта лежат в закладках браузера или телефона, и вы знаете, что заходить туда теперь будете оттуда, а не по ссылке из письма.

Пишет знакомый — а на самом деле его взломанный аккаунт

Тот же приём цепляет не только через письма, но и через мессенджер: взламывают аккаунт знакомого человека, а дальше пишут от его имени — обычно с просьбой срочно перевести денег, «неудоб-

но сейчас звонить». Узнавать почерк того, кто пишет, здесь бесполезно — пишет не он, а тот, кто получил доступ к переписке. Правило то же самое, что и с подозрительным письмом от банка: не отвечать в том же чате, а позвонить — человеку, а не в мессенджер, на тот номер, что уже есть в контактах. Настоящий знакомый ответит на звонок и подтвердит или опровергнет просьбу за один вопрос; если трубку не берут, а деньги нужны «прямо сейчас» — это уже само по себе повод не переводить.

Второй вариант той же схемы — не деньги, а сам аккаунт: пишут от имени «поддержки» мессенджера и просят продиктовать код, который придёт в СМС или в самом приложении, — под предлогом проверки, разблокировки или переезда на новое устройство. Этот код — то же самое, что пароль, только одноразовое: его не называют никому и никогда, ни «поддержке», ни знакомому, каким бы срочным ни казался повод, — у настоящей поддержки мессенджера этот код и так есть, спрашивать его незачем. Тот же принцип держит и «Облачный пароль» в Telegram из темы про двухфакторную аутентификацию: второй замок работает только до тех пор, пока его секрет знаете вы одни.

Сомневаетесь — звоните, а не отвечайте

Иногда решить с одного взгляда не получается: письмо выглядит убедительно, а срочность настоящая. Второй канал проверки — телефон, причём не тот номер, что указан в самом письме (его тоже мог вписать кто угодно), а тот, что напечатан на обратной стороне вашей карты или указан на официальном сайте, куда вы зашли сами. Звонок по этому номеру занимает пару минут и снимает вопрос целиком: настоящий банк подтвердит или опровергнет письмо за один вопрос оператору.

Записать номер стоит прямо сейчас, пока карта под рукой, а не в момент, когда придёт то самое письмо и разбираться будет уже некогда: переверните карту, наберите номер с обратной стороны в контакты телефона и подпишите понятно — «Банк, поддержка».

Тот же самый приём работает и для звонка, только теперь торопят голосом, а не письмом: звонят и представляются службой без-

опасности банка, просят «перевести деньги на резервный счёт» или продиктовать код из СМС, который только что пришёл. Здесь работает ровно то же правило: положить трубку и перезвонить самому — на тот номер, что записан в контактах с обратной стороны карты, а не на тот, с которого только что звонили и который удобно перезвонить прямо сейчас. Настоящий банк не обидится на этот лишний звонок; поддельный — не переживёт его, потому что ему нечего ответить настоящей службе поддержки.

Получилось — когда в контактах есть номер банка, переписанный с обратной стороны карты, а не найденный в письме или через поиск.

Максимум

На публичном Wi-Fi — в кафе, аэропорту, гостинице — к обычному фишингу добавляется ещё один сценарий: подмена происходит не на уровне письма, а на уровне самой сети. Первый признак — предупреждение браузера о сертификате: страница сообщает, что подключение не защищено или сертификат не подтверждён. Через такое предупреждение никогда не стоит проходить кнопкой «всё равно продолжить», даже если сайт очень хочется открыть прямо сейчас, — в этот момент браузер буквально не может подтвердить, с кем вы разговариваете. (☒ атака посредника). Второй признак — страница-заглушка, которая просит войти в сеть: часть таких страниц безобидна (гостиничный Wi-Fi иногда просит просто адрес почты), но если заглушка просит именно пароль от настоящей почты, а не что-то придуманное на ходу, — это уже не авторизация в сети, а форма для сбора паролей, наряженная под неё.

Проще всего оба сценария закрывает одна привычка: важные дела — банк, почта, оплата — на публичном Wi-Fi просто не делать. Переключитесь на мобильный интернет на те пару минут, что нужны для входа, а к Wi-Fi вернитесь потом, для всего остального.

- ☐ На публичном Wi-Fi войти в банк или почту не через сеть, а переключившись на мобильный интернет.

Если уже нажали и ввели пароль

Если это всё-таки случилось — сначала выдохните. Попадаются все, и чаще всего дело не в глупости, а в подгаданном моменте.

Шаг первый — сменить пароль на том сайте, куда он ушёл, и только после успеха обновить существующую запись в базе KeePassXC, которую вы завели в теме про пароли.

1. Откройте сайт через свою закладку или официальное приложение, а не через письмо, и откройте форму смены пароля, не вводя новый пароль вручную.
2. В KeePassXC откройте существующую запись этого сайта и запустите `Password Generator` / `Генератор паролей`.
3. Сгенерируйте пароль и проверьте оценку не ниже `100 bit`, затем скопируйте его и передайте только на официальный сайт.
4. Дождитесь подтверждения успешной смены пароля сайтом. Не сохраняйте запись заранее: в базе не должен остаться пароль, который сайт не принял.
5. После подтверждения замените значение в поле `Password` / `Пароль` существующей записи этим сгенерированным значением и нажмите `Save` / `Сохранить`. Не создавайте вторую запись.
6. Выйдите из аккаунта и проверьте новый вход по закладке, используя сохранённые логин и пароль.
7. После проверки нажмите `Clear Clipboard` / `Очистить буфер обмена`. Результат: вход успешен, а существующая запись содержит актуальный пароль.

Шаг второй — выгнать того, кто мог войти по старому паролю раньше, чем вы его сменили: смена пароля новый вход не пускает, но уже открытую чужую сессию сама по себе не закрывает, а второй фактор, если он был выключен в момент утечки, тоже её не тронет.

Gmail: выйти со всех чужих сеансов и проверить следы взлома

1. Откройте аккаунт Google ☒ «Безопасность и вход» ☒ блок «Ваши устройства» ☒ «Управлять всеми устройствами»: видно каждое устройство с открытым входом, и на любом из них,

кроме своего, можно нажать «Выйти».
2. Внизу главной страницы Gmail есть строка о последней активности аккаунта со ссылкой «Подробнее» — откройте её: там видно, если аккаунт открыт ещё где-то, и оттуда можно закрыть доступ везде разом одним действием, даже там, где Google не опознал устройство как чужое.
3. Шестерёнка вверху справа ⊠ «Все настройки» ⊠ вкладка «Пересылка и POP/IMAP»: проверьте, не появился ли там чужой адрес для пересылки писем, — это первое, что добавляют, чтобы читать вашу почту и после смены пароля. Нашли чужой — удалите.
4. Там же — вкладка «Фильтры и заблокированные адреса»: иногда вместо пересылки заводят фильтр, который молча архивирует или удаляет письма от банка, чтобы вы не заметили предупреждений. Удалите всё, чего не заводили сами.
5. В той же «Безопасности и входе» проверьте резервный телефон и почту для восстановления доступа: если их подменили, вернуть аккаунт станет сложнее даже тогда, когда пароль уже снова ваш.

Официально: устройства в аккаунте Google, пересылка писем, фильтры.

То же самое для Telegram: в настройках приложения есть раздел с активными сеансами (устройствами) — «Настройки» ⊠ «Устройства» или «Конфиденциальность» ⊠ «Активные сеансы», в зависимости от версии, — и там есть способ закрыть доступ на всех сеансах разом, кроме телефона в руках: занимает секунд десять.

Шаг третий — если это касается банка или карты, а тем более если деньги уже ушли. Позвоните по тому самому номеру с обратной стороны карты и расскажите, что произошло: банк умеет заблокировать карту или операцию быстрее, чем вы успеете придумать, как объяснить ситуацию покрасивее. Если деньги уже списались — то же самое, только быстрее и с одним уточнением: попросите не просто заблокировать карту, а отменить или вернуть сам перевод — банк не обязан это гарантировать, но шанс есть, только пока операция не обработана до конца, и он тает не по дням, а по часам, так что звонить стоит в тот же день, не откладывая на «сначала успоко-

юсь». Саму поддельную страницу тоже можно сдать — через форму Google «Сообщить о фишинговой странице»: вам лично это не поможет, зато с чуть большей вероятностью остановит следующего, кто откроет ту же ссылку.

Три шага, по порядку, спокойно и без ничего похожего на выговор самому себе.

Из всего фишинга в сухом остатке — одна привычка: важные места открывать своим путём, через закладку, а не по ссылке из письма. Стопроцентной гарантии это не даёт — рано или поздно можно ошибиться и каким-то другим путём, — но именно эта привычка одним действием закрывает подавляющее большинство случаев, без разбора каждого конкретного письма. А про то, как не потерять фотографии, документы и саму базу паролей, если что-то всё-таки случится, — тема про резервные копии: она не про то, как не попасться, а про то, что случившееся всё равно можно откатить назад.

Резервные копии

Телефон гораздо чаще не взламывают, а роняют в раковину, оставляют в такси или просто разбивают — и десять лет фотографий пропадают без единого хакера. Резервная копия ничего из этого не предотвращает: она просто гарантирует, что после случившегося у вас всё ещё есть файлы, а не разговор о том, что могло бы быть, — и это отдельный, честный жанр защиты.

Сделай это прямо сейчас

- ☐ Проверить, включено ли на телефоне облачное резервное копирование — 5 минут
- ☐ Включить на компьютере автоматическое копирование на внешний диск — 5 минут
- ☐ Скопировать базу паролей куда-нибудь ещё, кроме компьютера — 5 минут
- ☐ Найти, где лежат ваши фотографии, и убедиться, что они не только в телефоне — 5 минут

Три копии, два носителя, одна не рядом с вами

Правило трёх копий звучит как считалка, но в ней ровно три числа, и все три важны. Нужно минимум три экземпляра данных — включая рабочий, которым вы пользуетесь каждый день. Они должны находиться минимум на двух разных типах носителей, и минимум один экземпляр — вне дома или текущего места. Отдельно нужна хотя бы одна офлайн-копия: носитель должен быть отключён и недоступен для случайного удаления или шифровальщика. Вне

дома и офлайн могут быть разные копии.

Вот как эти три числа выглядят на живом примере — фотографиях за десять лет. Первый экземпляр — в самом телефоне, тот, которым вы пользуетесь каждый день. Второй — в облаке, куда телефон отправляет снимки сам. Третий — папка на внешнем диске, который раз в неделю подключается к компьютеру и снова уезжает в ящик стола. Три экземпляра; два разных вида носителя — память телефона и магнитный диск, а облако идёт третьим: облако лежит не там, где вы, а диск в ящике не подключён ни к чему постоянно. Облако выполняет условие «вне дома», а диск в ящике — условие «офлайн». Всё остальное в этой теме — про то, как включить каждый из этих трёх пунктов по отдельности.

Проверь себя. Все ваши фотографии за десять лет лежат в телефоне, и больше нигде. Сколько у вас копий этих фотографий? Напишите цифрой или словом.

Ноль. Единственный экземпляр — это не копия, это оригинал без страховки: он уезжает вместе с телефоном в такси, в воду и в чужой карман. Копия начинается со второго места хранения, а правило трёх копий говорит, что мест должно быть три, и одно из них — не там, где вы.

База паролей должна пережить компьютер

База KeePassXC особенно важна для резервной копии: пароли внутри неё не помнит никто, включая вас самих, а без мастер-пароля файл не откроет и сама программа. Поэтому рабочий файл не должен быть единственным экземпляром на компьютере.

Копия базы KeePassXC

1. В KeePassXC сохраните изменения, выберите `Database` / `База данных` -> `Lock Database` / `Заблокировать базу данных` и закройте программу.
2. Скопируйте именно файл `.kdbx` на отдельный носитель или в доверенное облако. Не экспортируйте базу в CSV/XML: такие файлы не защищены шифрованием базы.

3. Если используется key file, скопируйте и его, но в отдельное место, не рядом с единственной копией `.kdbx`. Мастер-пароль храните отдельно от обоих файлов.
4. Результат: есть рабочая база, отдельная копия `.kdbx` и, при необходимости, отдельная копия key file.

Восстановление и проверка

1. На проверочном устройстве откройте `Open Existing Database` / `Открыть существующую базу` и выберите копию `.kdbx`.
2. Введите мастер-пароль и, если он нужен, укажите key file. Не заменяйте рабочую базу восстановленной копией до проверки.
3. Откройте несколько групп и записей, сравните названия, логины, заметки и ожидаемые изменения. Для проверки key file закройте базу и повторите открытие с паролем и key file.
4. Результат: копия открывается, записи читаются, а единственная резервная копия не была отредактирована.

Что жалко потерять по-настоящему

Рабочий документ можно запросить заново у коллеги. Десять лет фотографий с телефона — уже нет, взять их больше неоткуда. Документы вроде сканов паспорта или договоров стоят на ступеньку ниже: восстановить их обычно можно, просто через отдельный поход в нужную организацию и потерянное время.

База паролей KeePassXC из темы про пароли стоит особняком. Это потеря, которую не восстановит никто и ничто: пароли внутри неё не помнит никто, включая вас самих, а без мастер-пароля файл не откроет и сама программа. Потерять эту базу без копии — значит начинать с нуля сразу по всем сайтам, которые в неё сложены.

Проверить, где на самом деле лежат фотографии, — минутное дело, но универсального «значка облака» у снимка не существует: в двух главных галереях проверка устроена по-разному, и в одной из них значок означает не то, что подсказывает интуиция.

Google Фото: значок в углу миниатюры и общий статус

1. Откройте «Google Фото» и найдите любой снимок годовой давности.
2. Посмотрите в правый нижний угол миниатюры. Значок резервного копирования стоит у тех снимков, которые уже уехали в облако, — логика здесь обратная привычной: значок означает «копия есть», а не «копия качается». Нет значка — этот конкретный снимок существует в одном-единственном экземпляре.
3. Общий статус — по фото профиля в правом верхнем углу: приложение прямо там пишет, всё ли скопировано, сколько ещё осталось загрузить или что копирование выключено вовсе.

Официально: как проверить резервное копирование.

iPhone: статус всей медиатеки, а не значок у снимка

1. Значка у отдельного снимка в «Фото» на iPhone нет вовсе — искать его бесполезно, статус здесь только общий, сразу на всю медиатеку.
2. Откройте «Фото» и нажмите кнопку профиля: статус библиотеки показан под именем — синхронизировано всё или загрузка ещё идёт.
3. В iOS 17 и раньше то же самое лежит в другом месте: вкладка «Медиатека», раздел «Все фото», и прокрутить в самый низ — статус синхронизации написан там, под последним снимком.

Официально: синхронизация фото с iCloud.

Если копии нет, чинить это поштучно не нужно: включить автозагрузку целиком проще, чем спасать снимки по одному, — и как раз про это следующий раздел.

Получилось — когда вы точно знаете: пропади телефон прямо сейчас, фотографии всё равно останутся — в облаке, на компьютере или там, где вы сами решили держать копию.

Телефон бэкапит себя сам — но не всё

На современном телефоне резервное копирование почти всегда уже встроено, хотя обычно это два разных переключателя, а не один: отдельно — копия самого устройства (настройки, контакты, данные приложений), отдельно — синхронизация фотографий. На iPhone оба живут рядом: «Настройки», затем имя профиля вверху, затем «iCloud», где «Резервная копия iCloud» отвечает за первое, а пункт «Фото» — за второе. На Android эти два переключателя разведены не просто по разным экранам, а по разным приложениям — и это главная причина, по которой человек уверен, что «бэкап включён», а фотографий в облаке при этом нет.

Android: копия самого телефона — на Pixel и на Samsung

1. Чистый Android и Pixel: «Настройки» ⊠ «Google» ⊠ «Резервное копирование». Там же есть кнопка «Начать копирование» — нажмите её один раз, чтобы не ждать ночи. То же самое открывается из приложения Google One: «Хранилище» ⊠ «Управление резервными копиями».
2. Samsung (One UI): путь другой — «Настройки» ⊠ «Учётные записи и архивация» ⊠ «Резервное копирование данных», это копия в Samsung Cloud. Уезжает она сама раз в сутки, но при трёх условиях разом: телефон на Wi-Fi, стоит на зарядке и не меньше часа лежит с погашенным экраном. То есть ночью и никак иначе.
3. Посмотрите, что там на самом деле лежит: копия телефона забирает данные приложений, журнал звонков, контакты, настройки и SMS. Фотографии в этом списке формально тоже есть, но отвечает за них отдельный переключатель из следующей плашки — включённой копии устройства для них недостаточно.
4. Бесплатных гигабайтов у Google пятнадцать, и они общие на почту, Диск и Фото разом. Это тот самый потолок, о котором ниже.

Официально: резервное копирование данных Android, то же для Pixel и как это устроено у Samsung — последняя страница на английском.

Android: автозагрузка фотографий — отдельный переключатель в Google Фото

1. Откройте приложение «Google Фото» — не «Настройки» телефона: этот переключатель живёт только здесь и больше нигде.
2. Нажмите на фото профиля в правом верхнем углу ⊠ «Настройки Google Фото» ⊠ «Резервное копирование».
3. Включите тумблер. Там же выбирается качество загрузки: исходное съедает бесплатные гигабайты быстрее всего, сжатое растягивает их надолго.
4. Убедитесь, что копирование пошло: на том же экране приложение показывает, сколько снимков осталось загрузить.

Официально: резервное копирование фото и видео.

Включить — не значит забыть насовсем. Бесплатного места у большинства сервисов немного — у iCloud это пять гигабайт, у Google пятнадцать, и те общие на почту, Диск и Фото, — а десять лет фотографий туда попросту не влезают: как только место кончается, копирование останавливается, а вместо рабочего бэкапа остаётся баннер «Хранилище заполнено», который легко не замечать месяцами.

Дальше начинается разговор про деньги, и подвох в нём не там, где кажется. Сами тарифы недорогие: у Google это 139 ₽ в месяц за 100 гигабайт, 219 ₽ за 200 и 699 ₽ за 2 терабайта (тарифы Google One); у Apple — 0,99 $ за 50 гигабайт, 2,99 $ за 200 и 9,99 $ за 2 терабайта. Мешает не сумма, а то, что заплатить её из России нечем: российские карты платёжный шлюз Google отклоняет, а пополнение баланса Apple Account с российских карт и через операторов отключено с апреля 2026 года. То есть бесплатные пять или пятнадцать гигабайт — это не стартовый тариф, с которого вы когда-нибудь съедете, а фактический потолок, если под рукой нет зарубежной карты.

Если платить за иностранное облако нечем: российское облако вторым местом

1. Встроенный бэкап телефона оставьте включённым: контакты, настройки и переписка умещаются в бесплатные гигабай-

ты спокойно. Место съедают фотографии — значит, уводить в другое облако нужно именно их.
2. Поставьте на телефон приложение Яндекс Диска или Облака Mail.ru: оба оплачиваются российской картой без плясок. Ориентир по цене — у Яндекса терабайт выходит около 4000 ₽ в год, два терабайта — около 600 ₽ в месяц; у Mail.ru платные тарифы начинаются примерно от 75 ₽ в месяц, бесплатно там дают 8 гигабайт.
3. Включите в самом приложении автозагрузку фотографий — она лежит в его собственных настройках, отдельно от настроек телефона, ровно как и у Google Фото.
4. Дождитесь окончания первой загрузки, затем подтвердите, что файлы доступны во втором хранилище, и сделайте тестовое восстановление. Не удаляйте фото обычным удалением из Google Фото или iCloud до этих проверок.
5. Для освобождения места используйте штатное действие сервиса: например, `Free up space` / «Освободить место» в Google Фото или оптимизацию хранилища iCloud. Эти действия освобождают место на телефоне или другом устройстве, но не уменьшают занятую облачную квоту. Если нужно освободить именно квоту, удаляйте копии из облака только после независимой копии и тестового восстановления: удаление может убрать фото из облачной библиотеки и с синхронизированных устройств. Название и доступность пункта могут отличаться в разных версиях.

Отдельная оговорка: переписка в мессенджерах в общий бэкап телефона обычно не попадает. У каждого своё резервное копирование, включается оно внутри самого приложения, и устроены они все по-разному — так что заглянуть придётся в каждый, которым вы всерьёз пользуетесь.

Telegram: копировать нечего, кроме секретных чатов

1. Ничего не включайте: обычные чаты Telegram и так живут в его облаке и появятся сами на любом новом устройстве, стоит туда войти. Здесь это уже сделано за вас, и это редкий случай, когда действий не требуется вовсе.
2. Исключение — секретные чаты. Они существуют только на

том телефоне, где заведены, исчезают вместе с ним и стираются при выходе из аккаунта. Скопировать их нельзя никак: если переписка из секретного чата важна, решение ровно одно — не держать её только там.

3. Свой архив выгружается с компьютера: Telegram Desktop ⊠ «Настройки» ⊠ «Продвинутые настройки» ⊠ «Экспорт данных Telegram». На выходе — папка с перепиской в JSON или HTML и с вложениями, которую дальше кладут туда же, куда и всё остальное.

Официально: про экспорт данных — страница на английском.

WhatsApp: включить копию и обязательно её зашифровать

1. «Настройки» WhatsApp ⊠ «Чаты» ⊠ «Резервная копия чатов». Копия уходит на Google Диск (Android) или в iCloud (iPhone) — то есть в те же бесплатные гигабайты, за которые уже идёт борьба выше.
2. Включите расписание — ежедневно или еженедельно. Вручную об этом не вспоминают никогда, это проверено на всех.
3. Там же найдите сквозное шифрование резервной копии и включите его: по умолчанию оно выключено, а это значит, что содержимое копии технически доступно Google или Apple, а не только вам.
4. Запирается оно паролем или 64-значным ключом — и пароль сразу в базу KeePassXC из темы про пароли. Забудете — копию не откроет никто, включая сам WhatsApp.

Официально: про сквозное шифрование резервных копий — страница на английском.

У Signal с февраля 2026 года есть свои Secure Backups — сразу на Android, iPhone и компьютере: бесплатно хранятся все текстовые сообщения и вложения за последние 45 дней, платно (около 2 $ в месяц) — до 100 гигабайт. Ключ восстановления там 64 символа, создаётся он на самом устройстве, и потерянный ключ не восстановит даже сама Signal, так что ему прямая дорога в базу паролей. Отдельно стоит знать, что обычная копия iPhone в iCloud переписку Signal не содержит вовсе: на Android у приложения есть свой файл резервной копии на самом телефоне, а на iPhone основные пути

— прямой перенос на новый телефон и то самое облачное Secure Backup. Эта часть Signal меняется от версии к версии чаще остального, так что смотреть стоит настройки той версии, которая стоит у вас сейчас.

Получилось — когда в настройках телефона напротив резервной копии устройства значится «Включено», а не «Предложить позже», и отдельно, уже в приложении галереи, включена автозагрузка фотографий. Это два разных «включено», и одного из них мало.

Внешний диск и автоматика на компьютере

Второй, устойчивый к другим бедам вид копии — внешний диск, который раз в неделю подключается, копирует файлы и снова убирается в ящик. Отключать его между копированиями — не паранойя, а главная причина, по которой такая копия справляется именно там, где облачная бессильна.

Диск под общие копии берут не тот же, что под пару мегабайт базы паролей из темы про пароли, и решает тут физика, а не цена. Флешка и внешний SSD держат данные зарядом, а заряд без питания медленно утекает — для носителя, который месяцами лежит в ящике отключённым, это ровно то свойство, которое не нужно. Обычный портативный жёсткий диск магнитный и этим не страдает; платите вы за это крутящейся механикой внутри, которая тоже не вечна, — но для копии в ящике размен правильный. Живые модельные ряды, которые несложно найти: Toshiba Canvio Basics, Seagate One Touch и Seagate Expansion, Western Digital My Passport и Elements — все портативные, питаются от того же USB-кабеля, которым подключаются, и отдельной розетки не просят.

Объём берите с запасом, а не впритык: правило большого пальца — вдвое больше того, что собираетесь копировать. Запас уходит не в воздух, а ровно на то, ради чего бэкап и нужен: на несколько копий разных дат, между которыми можно выбирать, и на то, что через два года данных станет больше. Домашний диапазон сегодня — два или четыре терабайта.

Дальше начинается то, на чём бэкапы обычно и заканчиваются: ко-

пировать папки руками раз в неделю вы будете ровно до тех пор, пока не забудете. И у macOS, и у Windows для этого есть штатная автоматика — настраивается один раз, после чего от вас требуется единственное движение: воткнуть диск.

Mac: Time Machine

1. Подключите диск к компьютеру.
2. Меню Apple ⊠ «Системные настройки» ⊠ «Основные» ⊠ «Time Machine» ⊠ «Добавить диск для резервного копирования». Выберите в списке свой диск.
3. При первом подключении macOS может предложить стереть диск — если на нём нет ничего нужного, соглашайтесь: под копии он нужен целиком.
4. Расписание настраивать не нужно, его попросту нет: Time Machine делает копию каждый час за последние сутки, ежедневную — за последний месяц и еженедельную за всё, что раньше. Когда место кончится, самые старые копии удалятся сами, без вопросов и без остановки копирования.
5. Шифрование по умолчанию выключено — это отдельная галочка «Зашифровать резервную копию» со своим собственным паролем. Нужна ли она вам, разобрано в блоке «Максимум» ниже.

Официально: как настроить Time Machine.

Windows: «История файлов» на внешний диск

1. Подключите диск.
2. Откройте «Панель управления» — именно её, старую: найдите по названию через поиск в меню «Пуск», в новых «Параметрах» этого пункта нет.
3. «Система и безопасность» ⊠ «История файлов». Windows сама увидит подключённый диск — нажмите «Включить».
4. Копироваться будут пользовательские папки — «Документы», «Изображения», «Музыка», «Видео», «Рабочий стол». Рядом, в «Дополнительных параметрах», настраивается, как часто снимать копию и сколько хранить старые версии.
5. Дальше всё идёт само, пока диск подключён. Отключённый диск «История файлов» просто ждёт и копирует, когда он вер-

нётся в порт.

Не перепутайте её с двумя соседями, которые называются похоже, а делают другое. «Резервное копирование Windows» («Пуск» ⊠ «Параметры» ⊠ «Учётные записи» ⊠ «Резервное копирование Windows») копирует примерно те же папки, но не на ваш диск, а в OneDrive, где бесплатно пять гигабайт, и требует учётной записи Microsoft — официальное описание. А «Архивация и восстановление (Windows 7)» в той же «Системе и безопасности» делает полный образ системы — штука полезная, но официально устаревшая много версий назад и живущая там скорее по инерции.

Отдельной системы под документы заводить не нужно — и когда тема про фишинг отправляет сюда за копией документов, она отправляет ровно к этому же диску. И Time Machine, и «История файлов» уже забирают те папки, где документы у большинства и лежат: «Документы» и «Рабочий стол». Сканы паспорта, договоры и рабочие файлы уезжают на диск тем же движением, что и всё остальное, никакого отдельного ритуала им не требуется.

Шифровальщик — вредоносная программа, которая шифрует файлы и требует денег за расшифровку, — при заражении добирается до всего, что подключено к компьютеру или доступно по сети: рабочие документы, папку с фотографиями, а заодно и внешний диск, если тот всё это время торчал в порту. До диска, который лежит отключённым в ящике стола, шифровальщик не доберётся при всём желании: он видит только то, что подключено прямо сейчас.

И ещё: копия, которую ни разу не проверяли, — это не гарантия, а надежда, что в нужный момент она сработает.

Получилось — когда файл базы паролей лежит ещё в одном месте, кроме компьютера, и вы можете назвать это место не задумываясь.

> **Максимум**
>
> Если внешний диск никуда не выезжает из дома, шифровать его — дело скорее вкуса: единственный риск, от которого спасает шифрование, — это кража или потеря самого диска, а дома этот риск невелик. Другое дело, если диск путешествует

вместе с вами — лежит в рюкзаке, ездит на дачу, иногда остаётся в машине: тут шифрование того стоит, потому что потерянный диск без шифрования читается на любом чужом компьютере как обычная флешка, а с шифрованием — как кусок бесполезного железа без вашего пароля.

Способ шифрования у Windows и Mac разный, и у обоих есть оговорки. В Windows нужен режим именно для съёмных дисков — BitLocker To Go, — а он доступен только в редакциях Pro и выше: в домашней редакции Windows такой диск можно прочитать, если его уже зашифровали на другом компьютере, но создать зашифрованный диск с нуля нельзя. На Mac обычный FileVault шифрует только системный диск самого компьютера, внешнего диска он вообще не касается — для внешнего диска нужен отдельный шаг: щёлкнуть по нему в Finder правой кнопкой и выбрать «Зашифровать…», либо переформатировать его в «APFS (зашифрованный)» через Дисковую утилиту. В обоих случаях дальше диск на каждом новом подключении спрашивает пароль — это не разовая настройка и не работа в фоне, хотя знакомый компьютер может запомнить пароль в своей связке ключей и не спрашивать его каждый раз.

Максимум

Копия, из которой ни разу не доставали файл, — это не копия, а надежда: она может годами исправно копироваться и оказаться битой именно в тот момент, когда понадобится по-настоящему, — а узнаете вы об этом только тогда.

Для файловой копии — внешнего диска, базы паролей — проверка занимает пять минут: откройте копию, найдите в ней одну случайную фотографию или документ и откройте файл — он должен открыться и оказаться тем же самым, что и на исходном устройстве. Так ловится именно битый файл: то, что один файл открылся, ещё не значит, что скопировалось вообще всё, — но для первой проверки этого достаточно.

Для облачного бэкапа телефона тот же трюк не сработает: он хранится единым образом устройства и разворачивается только целиком, при восстановлении на новый телефон, — вытащить из него один файл нельзя. Ближайшая честная замена — открыть облачную фотогалерею (icloud.com или Google Фото) с чужого устройства и увидеть там свои снимки; если совсем точно, это проверка того, что фотографии успевают синхронизироваться, а не самого бэкапа устройства, но за пять минут и без запасного телефона под рукой большего не проверить.

- ☐ Достать из резервной копии один файл и открыть его — убедиться, что копия действительно рабочая.

Почему это касается и вас, а не только компаний

Шифровальщики раньше были прежде всего темой для служб безопасности крупных компаний — целились туда, где можно потребовать выкуп посерьёзнее. Это давно не так: атаки давно не выбирают жертву по размеру, и обычный ноутбук с фотографиями и рабочими документами интересует их ровно так же, как сервер компании, лишь бы было чем шантажировать.

От заражения защищают антивирус, обновления и осторожность с незнакомыми вложениями — но ни один из них не даёт полной гарантии. Резервная копия устроена иначе: она не мешает шифровальщику добраться до файлов, зато делает саму атаку бессмысленной. Стёрли, зашифровали, потребовали денег — а у вас всё это время лежит отдельная копия, до которой он не дотянулся, и разговор с вымогателем можно вообще не начинать.

Это и есть другой жанр защиты. Почти все остальные темы бюллетеня учат не пускать беду внутрь; бэкап устроен иначе — он ничего не предотвращает и работает только после того, как беда уже случилась, — а к этому моменту она перестаёт быть катастрофой.

Максимум

Тема неприятная и потому откладывается навсегда: что будет

с фотографиями и документами, если с вами что-то случится, а доступ к ним понадобится близким. Решается это без завещаний и юристов — парой строк на бумаге рядом с мастер-паролем из темы про пароли: где лежит копия и как до неё добраться. Написать один раз и больше не возвращаться к этой мысли — задача именно такая, а не повод для тяжёлого разговора.

Копировать вручную вы будете старательно первую неделю, потом уже через раз, а там и вовсе забудете, — и дело не в характере, а в том, что так устроен буквально любой человек. Поэтому самый важный шаг из блока в начале — не разовое действие, а переключатель автоматики: включили один раз, и дальше телефон копит фотографии сам, а на вашей памяти остаётся только не забыть раз в неделю подключить диск для того, что в облако не попадает. А если из всего бюллетеня выбирать потерю, которую не восстановит никто и ничто, это база паролей без единой копии: пароли, которые не помнит никто, включая вас, вместе с файлом исчезают без следа. В следующей теме — про безопасность при использовании ИИ: разговор смещается с дисков и телефонов на то, что вы сами рассказываете чат-ботам.

Безопасность при использовании ИИ

То, что раньше служило доказательством — «я узнал этот голос, значит, это правда он», — сегодня подделывается за пару минут. Бдительность тут нужна того же сорта, что и в теме про фишинг: галочку один раз не включишь, каждый звонок оценивается заново.

Сделай это прямо сейчас

- ☐ Договориться с близкими о контрольном слове — 5 минут
- ☐ Условиться дома: деньги — только после обратного звонка на известный номер — 2 минуты
- ☐ Пролистать историю переписки с чат-ботом и удалить оттуда личные данные — 5 минут

Голос в трубке — больше не доказательство

Схема «звонит родственник, у него беда, срочно нужны деньги» знакома, наверное, всем — и раньше от неё худо-бедно спасала обычная внимательность: голос в трубке звучал слишком глухо, слова были не те, что сказал бы именно этот человек. Разница в том, что для убедительной подделки голоса сегодня хватает буквально пары минут любой записи этого человека — голосового сообщения, кружка в мессенджере, старого видео с чьего-нибудь дня рождения, — и результат звучит достаточно похоже, чтобы обмануть на слух в первые растерянные секунды звонка.

Отсюда неудобное следствие: голос в трубке больше не доказатель-

ство того, что говорит именно этот человек, — и видеозвонок, если честно, тоже, с картинкой умеют делать то же самое. Доказательство теперь ровно одно: перезвонить самому, на номер, который вы знаете заранее и набрали сами, а не тот, с которого только что звонили или писали, — тот же приём, что уже пригодился в теме про фишинг: доверяем каналу, который завели сами, а не тому, что подсовывают прямо сейчас. Тот же принцип касается и картинки: сгенерированная фотография или видео сами по себе ничего не доказывают, особенно если вас в этот момент ещё и торопят: спешка здесь не случайность, а часть схемы.

Получилось — когда дома есть чёткая договорённость: деньги переводятся только после звонка на номер, который вы набрали сами, а не тот, с которого только что звонили.

Контрольное слово: семейная игра, а не протокол

По-настоящему помогает тут контрольное слово внутри семьи. Придумать его можно прямо за ужином: кто-то в шутку предлагает «пусть будет фиолетовый бегемот» — и вот оно, слово готово; чем нелепее и своевольнее, тем лучше, лишь бы не имя питомца из соцсетей и не девичья фамилия бабушки, которые постороннему нетрудно найти. Это не протокол безопасности, а скорее семейная игра, и относиться к ней стоит именно так — паранойи в этой теме и так хватит без нашей помощи.

Договориться о слове — дело одного вечера, а вот пользоваться им приходится каждый раз заново, совсем как с приёмами из темы про фишинг: разового решения тут не бывает, каждый звонок оценивается отдельно. Даже если слово названо верно, для перевода денег обратный звонок на известный номер всё равно обязателен — это правило без исключений, слово его не заменяет; зато оно помогает решить, стоит ли вообще напрягаться с перезвоном, когда просьба не про деньги. И ещё стоит заранее проговорить вслух: спрашивать слово — не обидно и не значит «я тебе не верю», а если собеседник в трубке торопит и путает слово или не помнит его вовсе, вежливо вешайте трубку и перезванивайте сами, на тот номер, который знаете заранее.

Получилось — когда контрольное слово придумано и о нём знают все, кого оно касается, а не только вы один.

Что не стоит отправлять чат-боту

Список короткий: пароли, паспортные данные, медицинские выписки, финансовые документы, рабочие документы, чужие переписки. Правило одно на весь список сразу: всё, что вы отправили в чат-бот, вы отправили в чужую компанию, — а дальше это живёт по её правилам, а не по вашим.

Это очень болтливый попутчик в поезде: умный, полезный, охотно помогает, и совершенно точно перескажет ваш разговор дальше — не со зла, просто такой уж он есть. С этим попутчиком прекрасно обсудить, чем вирус отличается от червя, а вот паспорт ему в руки лучше не давать: да, заполнить анкету от руки и правда дольше, чем сфотографировать документ и переслать боту, — но у такого длинного языка доверия быть не может. (⊠ утечки данных).

Видео: Первый отдел (@DeptOne) — Чем ОПАСНЫ нейросети для взрослых https://www.youtube.com/watch?v=ADDePg3ty60

Первый отдел (@DeptOne) — Чем ОПАСНЫ нейросети для взрослых — подсказка к практике не отправлять нейросетям секреты и документы.

- 8:18 — утечки данных
- 13:31 — защита

Проверь себя. Что из этого лучше не отправлять в чат-бот? Отметьте всё, что подходит.

1. Просьбу объяснить своими словами, чем отличается вирус от червя.
2. Фотографию паспорта, чтобы бот заполнил за вас анкету.
3. Выписку от врача, чтобы бот пересказал диагноз человеческим языком.
4. Кусок рабочего договора, чтобы бот сделал из него короткое резюме.

Второй, третий и четвёртый. Правило простое: всё, что вы отправили в чат-бот, вы отправили в чужую компанию, на чужие серверы, и дальше это живёт по её правилам, а не по вашим. Первый вопрос — ровно то, для чего эта штука и нужна: спрашивать объяснения не жалко. А анкету, к сожалению, придётся заполнить руками — да, дольше.

Если что-то из списка уже отправлено — не поздно почистить задним числом: откройте историю переписки с чат-ботом (обычно она хранится прямо в приложении или на сайте, во вкладке с историей чатов) и сотрите те сообщения, где мелькали пароль, документ или чужие данные, — заодно и вложенные файлы, если вы их туда прикладывали.

Получилось — когда в истории переписки с ботом не осталось ни одного сообщения с паролем, документом или чужими данными.

Максимум

У большинства крупных чат-ботов есть отдельный переключатель, который управляет ровно одним: используют ли ваши переписки, чтобы дальше обучать модель. Живёт он почти всегда в одном и том же месте — в настройках аккаунта или приложения, в разделе про приватность или про данные, часто рядом с пунктом «история чатов»; конкретное название и путь у каждого сервиса свои и время от времени меняются, поэтому проще один раз самому открыть настройки и поискать слово «обучение» или «данные», чем полагаться на инструкцию, которая устареет раньше, чем вы её дочитаете.

Важно понимать, чего этот переключатель не делает. Он не удаляет уже отправленные сообщения с серверов компании — переписка там всё равно хранится какое-то время, обычно по своим правилам хранения. И он не превращает сервис в приватный: компания всё ещё видит, что вы ей написали, просто обещает не использовать это как учебный материал для будущих версий модели. Разница ощутимая, но не абсолютная — выключенный переключатель не повод присылать боту то, что туда и так отправлять не стоит: пароли, документы, чужие пе-

переписки. (☒ защита от утечек).

- ☐ Найти в настройках чат-бота пункт про обучение на ваших переписках и выключить его.

Уверенный тон — не то же самое, что правильный ответ

Уверенный тон ответа не означает, что ответ правильный. Модель не знает, что ошибается, — уверенность в тоне ничего не говорит о том, права она или нет, и неправильный ответ поэтому звучит ровно так же гладко, как правильный: так эта штука устроена по умолчанию, а не в редком сбойном случае. Проверять стоит именно там, где на кону деньги, лекарства и документы, а не в любом случае подряд — если бот помогает накидать вариантов подарка на день рождения, лишняя проверка попросту не нужна.

Максимум

Есть способ вообще не пересылать свои данные никакой компании — запустить языковую модель локально, на собственном компьютере, без интернета и без чужих серверов в цепочке. На практике это означает установить отдельную программу (например, LM Studio или Ollama) и загрузить в неё файл модели размером в несколько гигабайт — дальше разговор происходит только между вами и вашим же компьютером.

Дальше начинаются оговорки. Модели, которые тянет обычный домашний компьютер без мощной видеокарты, заметно слабее и медленнее тех, что крутятся на серверах крупных компаний, — и это честный компромисс, а не бесплатный обед. Локальная модель — вариант для тех, кому конфиденциальность конкретной задачи важнее качества и скорости ответа: юриста с чужими документами, врача с историями болезни, кого угодно, кто по работе регулярно имеет дело с чужими секретами, а не разово. Для обычной бытовой переписки с ботом — спро-

> сить рецепт или помочь с письмом — овчинка обычно не стоит выделки: обычный веб-сервис с выключенным обучением на переписках справится ничуть не хуже и без возни с установкой.

Если сводить тему к одной мысли: раньше, чтобы убедительно обмануть, нужно было постараться, а теперь для этого хватает пары минут случайной записи и чужой спешки, — поэтому и защита работает не на слух, а на действии: контрольное слово заранее и обратный звонок на известный номер, когда что-то не сходится. В следующей теме — про приватность в сети: разговор смещается с того, что вы сами присылаете в чат, на то, что о вас и так видно посторонним в браузере и в соцсетях.

Приватность в сети

Эта тема — скорее гигиена, чем острый риск: если с вами вдруг случится что-то неприятное в сети, причина почти наверняка окажется не в отсутствии блокировщика рекламы. Зато окупается всё это сразу — в тот же день реклама и слежка в браузере заметно стихают, а на собственной странице в соцсети находится что-нибудь неожиданное.

Сделай это прямо сейчас

- ☐ Поставить в браузер блокировщик рекламы и трекеров — 3 минуты
- ☐ Выбрать защищённый мессенджер и написать в нём одному человеку — 5 минут
- ☐ Открыть свою страницу в соцсети от чужого имени и посмотреть, что видно — 7 минут

Блокировщик — единственное изменение в браузере с такой отдачей

Из всего, что творится в браузере, блокировщик рекламы и трекеров — редкий случай, когда безопасность не требует компромисса с удобством: интернет после установки становится ощутимо тише и быстрее, а безопаснее получается просто попутно. Не жертва, а подарок.

Реклама с сомнительными баннерами и всплывающими окнами перестаёт показываться вовсе, а вместе с ней часто пропадают

и вредоносные баннеры, через которые иногда пытаются подсунуть что-нибудь неприятное даже на совершенно обычном, безобидном сайте. А трекеры — небольшие невидимые скрипты, которые в обычном режиме следят, на какие сайты вы заходите, и складывают эту историю в профиль, который потом продают рекламодателям, — просто перестают загружаться, и заодно страницы начинают открываться быстрее: браузеру больше не приходится вытягивать десяток чужих скриптов на каждую загрузку. Стопроцентной гарантии блокировщик не даёт — часть рекламы и трекеров всё равно просачивается, особенно там, где сайт специально с ним борется, — но перекрывает он подавляющее большинство, и разница заметна уже на первой открытой странице. (⊠ цифровой след после посещений).

Ставится блокировщик один раз. В Firefox это полноценный uBlock Origin из официального магазина расширений. В Chrome и Edge такого выбора больше нет — полную версию из них убрали, и доступна там только урезанная uBlock Origin Lite, тоже рабочий вариант, просто послабее. Какой бы блокировщик ни стоял, дальше он просто работает: изредка разве что приходится вручную разрешить рекламу на конкретном сайте, который без неё не работает.

Получилось — когда блокировщик стоит в браузере, а на привычных сайтах реклама и трекеры перестали появляться сами собой.

Остальная гигиена браузера

Дальше — список необязательных мелочей. Ни одна сама по себе погоды не делает, но вместе они снижают число следов, которые вы оставляете в сети просто по ходу обычных дел.

Отдельный профиль браузера — вещь, о которой многие даже не подозревают. В большинстве браузеров можно завести второй, полностью самостоятельный профиль — со своими закладками, паролями и историей, — и держать в нём то, что не хочется смешивать с основной жизнью в интернете: рабочую переписку, случайные регистрации на сайте, которым вы воспользуетесь один раз, или что угодно ещё, что удобнее вести отдельно. Заводится профиль в настройках браузера, в меню, где обычно и стоит

значок вашего аккаунта, — и дальше это ещё одно окно со своей собственной историей, а не отдельная программа.

Максимум

Тот же принцип «не смешивать» работает и с почтой. Есть смысл завести не один адрес на всё, а хотя бы два. Один — под по-настоящему важное: банк, госуслуги, рабочую переписку, восстановление доступа к другим аккаунтам. Второй — под всё остальное: регистрации в интернет-магазинах, рассылки, разовые скидки, форумы и сервисы, которыми вы, скорее всего, воспользуетесь один раз и забудете.

Смысл не в том, чтобы что-то скрыть, а в том, что рано или поздно база данных какого-нибудь случайного магазина утечёт в сеть вместе с вашим адресом и, возможно, паролем, — происходит это с пугающей регулярностью и почти никогда не зависит от того, насколько аккуратно вы сами себя вели. Если утечёт «магазинный» адрес, дальше по нему разве что придёт немного спама. Главный, важный адрес так и останется никому не известным по этой конкретной утечке.

- ☐ Завести отдельный почтовый адрес под регистрации в магазинах и рассылки.

Чистка данных сайтов — самая скучная часть этого списка и, кажется, поэтому и самая недооценённая: со временем в браузере накапливаются куки и локальные данные тысяч сайтов, на которых вы были один раз и давно забыли. Раз в несколько месяцев их стоит стирать в настройках браузера, в разделе про приватность и данные сайтов, — вы почти ничего не потеряете, кроме необходимости заново войти на паре сайтов, зато исчезнет годами копившийся хвост из данных, которые уже никому не нужны, кроме тех, кто их когда-то собрал. (☒ следы браузера), которые накапливаются в таких данных.

И последнее — поисковик, который не собирает историю запросов. Большинство поисковиков по умолчанию хранят каждый ваш за-

прос и привязывают его к вам; есть и такие, вроде DuckDuckGo, которые устроены иначе и просто не ведут эту историю. Сменить поисковик по умолчанию — разовая настройка в браузере. (☒ метаданные).

Видео: Первый отдел (@DeptOne) — Что выдаёт вас в интернете каждый день https://www.youtube.com/watch?v=QNDet8tKB3k

Первый отдел (@DeptOne) — Что выдаёт вас в интернете каждый день — подсказка к цифровым следам, геолокации, следам браузера и метаданным; не заменяет настройки выше.

- 7:31 — цифровой след
- 9:19 — геолокация
- 12:40 — следы браузера
- 15:29 — метаданные

Защищённая и незащищённая связь

Открытая (обычная) связь здесь означает не «видно всем в интернете», а «нет подтверждённого сквозного шифрования (E2EE) между устройствами». К ней относятся обычные личные облачные чаты Telegram, включая чат с самим собой, группы и каналы, SMS, обычная почта и любые чаты, в которых E2EE не заявлено и не проверено. Шифрование соединения до сервера само по себе не делает такую переписку сквозной.

Не пересылайте по открытым каналам пароли, TOTP и резервные коды, паспорта и другие документы, номера банковских карт и CVV, ключи восстановления, сканы и другие идентификаторы. Не отправляйте такие секреты даже «самому себе» в облачный чат: это всё равно ещё одна копия на серверах и устройствах. Пароли храните в KeePassXC, для разовой передачи используйте заранее проверенный безопасный канал, а получателя перепроверяйте другим каналом.

Минимум: Telegram Secret Chat

Если нужен именно Telegram и содержание личного разговора должно быть E2EE, используйте `Secret Chat` / `Секретный чат`. Откройте профиль контакта и выберите `Start Secret Chat` / `Начать секретный чат`. Убедитесь, что чат действительно помечен как Secret Chat, а не является обычным облачным чатом. Внутри при необходимости включите `Self-Destruct Timer` / `Таймер самоуничтожения`: он ограничивает срок хранения сообщений, но не отменяет остальные правила.

Secret Chat работает только для личного разговора. Это не защита для групп, каналов или обычных чатов. Такой чат привязан к устройствам, на которых его начали, и не синхронизируется как обычная облачная переписка. Telegram Secret Chat не скрывает метаданные и не делает пользователя анонимным. Предупреждение о скриншоте не гарантия: экран можно сфотографировать другим устройством или обойти такое предупреждение.

Даже Secret Chat не предназначен для передачи паролей, паспортов, документов и данных карт как обычной практики. E2EE защищает канал от перехвата, но не защищает от получателя, разблокированного или заражённого телефона, скриншота или уже скомпрометированного устройства.

Официальные материалы Telegram: FAQ о Secret Chats, как устроено шифрование, FAQ о скриншотах и FAQ о таймере самоуничтожения.

Защищённый мессенджер: что на самом деле означает сквозное шифрование

Сквозное шифрование — фраза, которую мессенджеры вставляют в рекламу так часто, что она почти перестала что-либо значить, а зря: смысл там простой. Если переписка зашифрована сквозным способом, прочитать её не может даже тот, кто её передаёт, — то есть сама компания, которой принадлежит мессенджер, физически не может открыть ваши сообщения, даже если получит на это официальный запрос. Устроено это так, что ключ для расшифровки есть только на двух устройствах — вашем и собеседника, — а

на серверах компании переписка всё это время лежит нечитаемым набором символов. У этой защиты есть и свой предел: она прячет содержимое переписки, а не сам факт, что вы с кем-то переписываетесь и когда, — и уж тем более не мешает собеседнику самому сделать скриншот и переслать его дальше.

Реализовано это у всех по-разному, и разница тут важная. У Signal сквозное шифрование включено по умолчанию для всех переписок без исключения — ничего дополнительно настраивать не нужно. У части других приложений такая возможность тоже есть, но не по умолчанию: обычная переписка идёт без сквозного шифрования, а чтобы его получить, нужно отдельно запускать особый, защищённый режим переписки для конкретного собеседника — и если вы этого не сделали, защиты нет, хотя по названию мессенджера может казаться, что она есть всегда. А часть популярных программ для переписки сквозного шифрования не делает вовсе, ни в каком режиме, — там сообщения в какой-то момент проходят через сервер компании в виде, который эта компания вполне может прочитать.

Максимум

На конкретном примере — мессенджере MAX, оператор которого, ООО «MAX», входит в холдинг VK, — нет публичного подтверждения сквозного шифрования или отдельного защищённого режима. Самое проверяемое написано в его же документах: политика конфиденциальности на legal.max.ru/pp не упоминает шифрование переписки ни одним словом — ни протокола, ни обещания, — нет такого описания и в остальных документах оператора. Это отсутствие публичного подтверждения, а не доказательство того, что шифрования нет в любом режиме. Поэтому не отправляйте через MAX чувствительные данные или секреты, если не доверяете сервису или его защита не подтверждена. Зато расписано другое: что собирается (данные регистрации, сведения об устройстве, IP, геолокация, журналы действий; с отдельного согласия — данные из Госуслуг) и кому передаётся — разработчикам мини-приложений и ботов, сотовым операторам-партнёрам, компаниям группы VK

и государственным органам «по официальным законным запросам». Это не обвинение, а оглавление документа, который лежит в открытом доступе.

Честности ради: разрешений MAX просит не больше конкурентов, а меньше — в независимом сравнении (замеры Exodus Privacy, разбор на Хабре) у него насчитали 59 против 72 у Telegram и 85 у WhatsApp, а с версии 25.11.0 — 50. Дело, стало быть, не в количестве галочек, а в сочетании: это не просто мессенджер, а платформа с входом через Госуслуги, мини-приложениями и платежами, которая о сквозном шифровании нигде не заявляет, а передача данных третьим лицам и государственным органам по законному запросу описана в её же политике. Появиться на телефоне он при этом мог и без вашего участия: с 1 сентября 2025 года MAX входит в список программ, обязательных для предустановки на продаваемые в России телефоны и планшеты.

Дальше по ситуации. Не нужен — удалить; предустановленное удаляется не всегда, и тогда рабочий вариант — отключить его в настройках приложений, чтобы не запускался и не обновлялся. Нужен по-настоящему — из-за работы, школьного чата или сервиса, который требует именно его, — не воевать, а изолировать: в отдельном рабочем профиле приложению достаются пустые контакты, пустые файлы и совсем другой список установленных программ вместо ваших, а как такой профиль завести, разобрано в теме про второе пространство на Android. VPN эту задачу не решает: он меняет только то, кто видит ваш трафик по дороге, и ничего не может поделать с тем, что установленное приложение читает прямо на устройстве — по разрешениям, которые вы ему сами и выдали.

- ☐ Удалить MAX с телефона (не удаляется — отключить), а если без него не обойтись — перенести его в отдельный рабочий профиль.

Signal и Session: защищённая переписка

Оба мессенджера используют сквозное шифрование (E2EE): содержимое сообщения должно быть доступно только участникам разговора. Это не обещание анонимности, невзламываемости или безопасности самого телефона. Шифрование также не подтверждает личность собеседника: можно надёжно зашифровать переписку не с тем человеком.

Максимум

Signal

В Signal E2EE включено по умолчанию для личных и групповых чатов. Установочный файл берите с официальной страницы или из официального магазина. Для регистрации нужен номер телефона, но это не делает Signal анонимным и не скрывает от всех сам факт использования сервиса.

В `Settings` / `Настройки` ☒ `Privacy` / `Конфиденциальность` включите `Registration Lock` / `Блокировка регистрации` и задайте `Signal PIN` / `Signal PIN`. PIN и `Registration Lock` / `Блокировка регистрации` защищают повторную регистрацию аккаунта, но это не 2FA и не замена паролю от телефона. Там же включите `Screen Lock` / `Блокировка экрана`. Регулярно проверяйте `Linked Devices` / `Связанные устройства` и удаляйте незнакомые.

Для важного контакта откройте карточку чата ☒ `View Safety Number` / `Просмотреть код безопасности`. Сверьте код лично или через другой доверенный канал и при совпадении нажмите `Mark as Verified` / `Отметить как проверенный`. Сам значок шифрования не доказывает личность.

`Disappearing Messages` / `Исчезающие сообщения` полезны как уборка истории, но не защищают от скриншота, фотографии экрана, копирования текста или записи другим устройством. Пароли, TOTP-секреты и резервные коды в чат не отправляйте.

Официальные материалы Signal: PIN, Screen Lock, Linked Devices, Safety Numbers, Disappearing Messages.

Session

Session не требует номера телефона или почты. При создании он генерирует случайный `Account ID` / `Account ID`. Устанавливайте приложение только с getsession.org/download. (☒ начало работы с Session). При создании аккаунта сразу запишите `Recovery Password` / `Recovery Password` (seed-фразу) на бумаге и храните отдельно от телефона; никому её не сообщайте. Это не обычный пароль и не 2FA.

Видео: Tech Talk (@TechTalk_NotDead) — Session – самый анонимный мессенджер? Как работают даркнет и сеть Oxen https://www.youtube.com/watch?v=i8_XzqJoFkc

Tech Talk (@TechTalk_NotDead) — Session – самый анонимный мессенджер? Как работают даркнет и сеть Oxen — подсказка к запуску и выбору Session; название не означает абсолютную анонимность.

- 4:50 — начало работы с Session
- 5:34 — обзор
- 9:46 — ограничения

Передавайте `Account ID` / `Account ID` отдельно и подтверждайте личность собеседника через второй канал. В Session используются E2EE, Onion Requests и Session Nodes, но отсутствие номера не означает абсолютную анонимность и не скрывает IP от всех. Доставка может задерживаться. Текущий Protocol V1 использует Long-Term Key и не даёт Perfect Forward Secrecy. (☒ ограничения Session).

Включите `Lock App` / `Блокировка приложения`. Исчезающие сообщения в Session, как и в Signal, только сокращают срок хранения в интерфейсе и не мешают скриншотам, фотографиям, копированию или пересказу. Восстановление аккаунта по Recovery Password не равно полному резервному копированию истории.

Официальные материалы Session: главная, загрузка, документация, FAQ, политика приватности.

	Signal	Session
Номер и почта	Нужен номер для регистрации	Не нужны
Идентификатор	Номер телефона и профиль	Случайный Account ID
Проверка контакта	Safety Number через другой канал	Account ID и личность через другой канал
Маршрутизация	Серверы Signal; содержимое E2EE	Onion Requests и Session Nodes; возможны задержки
Восстановление	Зависит от регистрации и доступных функций резервирования	Recovery Password/seed-фраза; не полный backup истории
Основные ограничения	Номер не даёт анонимности; экран можно сфотографировать	V1 без Perfect Forward Secrecy; отсутствие номера не даёт абсолютной анонимности
Подходящий сценарий	Удобный защищённый канал для проверенных контактов	Когда важна регистрация без номера и допустимы псевдонимность и задержки

Signal: базовый безопасный сценарий

1. Установите Signal с официального сайта или из магазина и зарегистрируйте номер.
2. В Settings / Настройки ⊠ Privacy / Конфиденциальность включите Registration Lock / Блокировка регистрации и Screen Lock / Блокировка экрана.
3. Важного собеседника проверьте через View Safety Number / Просмотреть код безопасности и другой канал, затем нажмите Mark as Verified / Отметить как проверенный.
4. Проверьте Linked Devices / Связанные устройства; неизвестное отключите. Disappearing Messages / Исчезающие сообщения включайте только как уборку.
5. Не отправляйте в чат пароли, TOTP-секреты и резервные коды.

Session: базовый безопасный сценарий

1. Установите Session только с getsession.org/download и выберите Create Account / Создать аккаунт.
2. Запишите Recovery Password / Recovery Password на бумаге и уберите отдельно; не называйте её 2FA или заменой полной резервной копии.
3. Передайте Account ID / Account ID отдельным каналом и подтвердите личность собеседника через второй канал. При восстановлении выберите I have an account / У меня уже есть аккаунт.
4. Включите Lock App / Блокировка приложения; Disappearing Messages / Исчезающие сообщения используйте лишь для уборки.
5. Учитывайте задержки, отсутствие Perfect Forward Secrecy в Protocol V1 и то, что восстановление аккаунта не возвращает автоматически всю историю.

☐ Создать аккаунт в Signal или Session, сохранить секрет восстановления вне чата и проверить одного собеседника через второй канал.

Итог выбора: Telegram Secret Chat — точечный режим внутри Telegram; Signal — удобный защищённый канал для проверенных контактов; Session — вариант, когда важна регистрация без номера и допустимы псевдонимность и задержки. Ни один из них не подходит для пересылки мастер-пароля, паспорта или данных карты как обычной практики.

Соцсети: взгляд на свою страницу глазами постороннего

Здесь не нужно ничего устанавливать — нужно на семь минут стать посторонним человеком и открыть собственную страницу в соцсети так, как её видит тот, кто вам не друг: в приватном окне браузера, не заходя в свой аккаунт, или попросив об этом кого-нибудь незнакомого с вашей страницей. Это не для того, чтобы ужаснуться, а скорее взгляд в зеркало заднего вида — увидеть не что-то новое, а то, что там уже давно видят все, кроме вас самих.

Смотреть стоит на четыре конкретные вещи: виден ли телефон, виден ли список друзей целиком, доступны ли старые фотографии за прошлые годы и написано ли где-то место работы. Ни один из этих пунктов не опасен сам по себе — соцсеть для того и нужна, чтобы её видели, — но у каждого есть настройка, которая решает, видит ли это первый встречный или только те, кому вы сами это показали. Разница между «настройка стоит по умолчанию» и «настройка выбрана осознанно» и есть весь смысл этих семи минут.

Получилось — когда вы посмотрели на свою страницу со стороны и увидели, что из этих четырёх вещей видно первому встречному, а что нет.

Максимум

Полный список того, где ваше имя и фотография уже когда-то засветились, обычно длиннее, чем кажется: старый форум, который вы забыли, что регистрировали, комментарий пятилетней давности под чужим постом, профиль на сайте,

которым вы пользовались один раз. Часть этого действительно можно убрать — написать в поддержку сервиса с просьбой удалить аккаунт, найти в настройках старой соцсети кнопку «удалить страницу», попросить владельца форума стереть отдельный пост. Часть — уже не убрать никогда: то, что кто-то успел скопировать или процитировать в другом месте, из первоисточника не исчезает вместе с исходной публикацией.

Полностью «исчезнуть» из интернета — цель нереалистичная, и это нормально: гнаться за ней не нужно. Настоящая, достижимая цель звучит куда скромнее — убрать то, что явно лишнее и давно не нужно, а не добиться нулевого следа. Разница именно в этом: не «обо мне в сети ничего нет», а «там нет того, чего там быть не должно».

Публичный Wi-Fi: что там реально опасно

Про публичный Wi-Fi в кафе или аэропорту существует расхожая страшилка: сосед за соседним столиком якобы читает вашу переписку прямо из эфира. Сегодня это по большей части уже не так — почти весь трафик в интернете и так зашифрован, и просто перехватить данные из воздуха стало заметно труднее, чем раньше (замочек в адресной строке и что он на самом деле доказывает, подробнее разобраны в теме про фишинг). Опасность не исчезла, а переехала в другое место.

Реальный риск на публичной сети — это подмена: поддельная точка доступа с похожим названием или страница-заглушка, которая просит «войти в сеть» и вместо простой авторизации спрашивает пароль от настоящей почты. Гостиничный или кафейный Wi-Fi иногда и правда просит представиться — адрес почты без пароля, — и это безобидно; но если заглушка настойчиво просит именно пароль, а не просто адрес, дело уже не в доступе к сети — под этим предлогом у вас просто пытаются выманить пароль от почты. Правило то же, что и с фишингом: заходить в банк и почту стоит своим путём, а не по ссылке или форме, которую подсунула сама сеть.

А что насчёт VPN? Невидимым он вас не делает и от всего сразу не

защищает — он меняет того, кому вы доверяете передачу трафика: без VPN это владелец сети, к которой вы подключились, то есть та самая кофейня, — с VPN это владелец сервиса VPN. Обоим технически доступно видеть, куда вы ходите, если очень захочется; разница только в том, кому вы больше доверяете. Поэтому в публичной сети, где нет доверенного варианта вообще, VPN может быть разумным выбором, а вот заменой внимательности к поддельным страницам и запросам пароля он не станет никогда.

Проверь себя. Вы в кофейне, подключились к бесплатному Wi-Fi, надо зайти в банк. Что действительно помогает?

1. Зайти по ссылке из письма от банка — оно как раз пришло.
2. Включить VPN и считать, что теперь вас не видит вообще никто.
3. Открыть банк из его приложения или из своей закладки.
4. Ничего не менять: замочек в адресной строке всё равно есть.

Третий. Замочек и правда шифрует канал, и старая страшилка «в кафе читают вашу переписку» сегодня почти неактуальна — опасность переехала. Теперь вас скорее попробуют увести на поддельную страницу или показать заглушку «войдите в сеть», просящую пароль от почты, а против этого помогает ровно одно: заходить своим путём. VPN тоже не плащ-невидимка: он меняет того, кто видит ваш трафик, — вместо кофейни это владелец VPN, которому надо доверять не меньше.

Если сводить тему к одной мысли: полная приватность в интернете — цель недостижимая, и гнаться за ней бессмысленно, а вот не оставлять больше следов, чем нужно, там, где это ничего не стоит, — вполне достижимая и по-настоящему полезная привычка. Блокировщик, взгляд на собственную страницу со стороны и один осмысленный разговор про мессенджер закрывают львиную долю того, что вообще можно закрыть за пятнадцать минут. В следующей теме — про выбор и проверку программ: разговор смещается с того, что о вас видно в сети, на то, откуда вообще берётся софт на ваших устройствах.

Выбор и проверка программ

Устройство ровно настолько безопасно, насколько безопасно то, что вы на него поставили. Самый надёжный пароль и вовремя обновлённая система ничего не изменят, если рядом с ними работает программа, которая когда-то попала на устройство с сомнительного сайта и с тех пор просто там и осталась.

Сделай это прямо сейчас

- ☐ Проверить, откуда скачана программа, которой пользуетесь чаще всего — 3 минуты
- ☐ Открыть список установленных программ и удалить три, которыми не пользуетесь — 10 минут

Магазин, сайт разработчика и первая строка в поиске — не одно и то же

Программа попадает на устройство разными путями, и они далеко не равноценны. Первый — встроенный магазин приложений: App Store, Google Play, Microsoft Store, магазин на Mac. Площадка там хоть как-то проверяет, что публикует, и умеет убрать программу задним числом, если та начинает вести себя плохо. Второй — официальный сайт разработчика: адрес, который вы набрали сами или взяли из проверенного источника, а не тот, что подвернулся первым. Есть и ещё один вариант, менее очевидный, но не менее надёжный: установка из репозитория — открытого каталога программ, который сам следит за обновлениями, а не оставляет это

вам. Любой из этих путей — нормальный выбор, и для большинства программ этого достаточно.

А есть путь, которым лучше вообще не пользоваться: случайная ссылка из результатов поиска. Верхние строчки выдачи обычно рекламные места, их покупают, и покупают их в том числе те, кто продаёт не архиватор, а вашу собственную машину под видом архиватора: та же иконка, то же название, а внутри — совсем другое. Поэтому самый надёжный способ поймать вредонос — вовсе не открыть подозрительный файл специально, а просто нажать на первую ссылку в поиске, не задумываясь, что это реклама, а не результат.

А если программа уже стоит на устройстве и вы просто не помните, откуда она взялась, источник тоже можно установить задним числом: если программа значится в магазине приложений — в разделе вроде «Библиотека» или «Мои приложения» (в Google Play это «Управление приложениями и устройством» ☒ «Управление» за значком профиля), — источник ясен сразу. Сам Android, увы, нигде не подписывает, из какого магазина в своё время поставлено конкретное приложение, так что если этот путь не сработал, стоит заглянуть в историю загрузок браузера: она хранит адрес страницы, с которой в своё время скачивался установочный файл, если, конечно, программа вообще пришла через браузер, а не была установлена как-то иначе.

> **Максимум**
>
> На практике репозиторий работает как одна большая подписка, а не разовая установка: устройство подключается к каталогу целиком, а дальше все программы из него обновляются пачкой, без единого отдельного скачивания. Это в первую очередь история Linux и Android, а не универсальный способ на все системы сразу: в Linux это вообще основной способ с самого начала, программы ставятся через приложение вроде «Центра приложений» — обычное окно со списком и кнопкой «Установить», никакой терминал для этого не нужен. На Android то же самое умеет F-Droid — каталог программ с открытым кодом,

из которого их можно ставить без магазина Google. У Windows и Mac прямого аналога с той же простотой нет: там магазин приложений — по сути и есть их версия репозитория, а остальное по-прежнему приходит отдельными файлами с сайтов.

Разница с обычным скачиванием не в удобстве, а в устройстве самого процесса. Файл с сайта — это снимок на момент скачивания: если завтра в программе найдут дыру, узнать об этом и поставить исправление — уже ваша забота. Программа из репозитория обновляется сама, вместе со всем остальным, что стоит рядом, и каждый раз приходит из одного и того же проверенного места, а не оттуда, куда вы в этот раз случайно попали.

Проверь себя. Нужен архиватор. Откуда его брать? Отметьте все разумные варианты.

1. С официального сайта программы, найденного не по рекламной ссылке в поиске.
2. По первой ссылке из поиска по запросу «скачать бесплатно без регистрации».
3. Из встроенного магазина приложений вашей системы.
4. Из открытого каталога программ, который сам присылает обновления.

Первый, третий и четвёртый. Разница между ними невелика, а вот второй пункт стоит особняком: первые строки в поиске продаются, и продают их в том числе тем, кто собирает не архиватор, а вашу машину. Отдельная тонкость про первый вариант — «официальный сайт, найденный не по рекламной ссылке»: рекламный блок сверху выдачи выглядит точно так же, как обычный результат, и ведёт куда угодно.

Получилось — когда вы точно знаете, откуда на устройстве взялась программа, которой пользуетесь чаще всего: из магазина приложений, с официального сайта или из репозитория, а не «непонятно откуда».

«Скачать бесплатно без регистрации и СМС» — самое дорогое предложение в интернете

Только платят за него не деньгами. Взломанная («бесплатная») версия платной программы работает по одной и той же схеме: чтобы обойти защиту от копирования, кто-то сначала должен залезть внутрь установочного файла и что-то в нём подправить, а раз файл уже открыт для правок, вместе с обходом защиты в него нередко подкладывают что-то ещё, что работает уже не на вас. Это давняя и хорошо изученная классика, а не редкий страшный случай: под угрозой не только сомнительные малоизвестные сборки, но и самые массовые взломанные версии популярных программ.

Дело не в законности, а в том, кто на самом деле правил файл, который вы ставите. Переписывал его не автор оригинальной программы, а кто-то третий, кого вы никогда не видели и не выбирали, а доверяете вы ему ровно так же, как доверяли бы автору. Если платить за программу не хочется или не на что — решение не в риске, а в замене: у многих платных программ есть открытый бесплатный аналог — LibreOffice вместо Microsoft Office, GIMP вместо Photoshop (там же, на странице загрузки, для каждого установщика сразу публикуют SHA-256 и ссылку на проверку файла в VirusTotal — ровно то, о чём разговор чуть дальше по теме) — или честная, пусть и урезанная, бесплатная версия от самого разработчика. Архиватор из примеров и квиза выше по теме тоже стоит назвать прямо, а не оставлять безымянным: это 7-Zip — бесплатный и с открытым кодом. Сами официальные ссылки на него ведут на страницу релизов проекта на GitHub (github.com/ip7z/7zip) — это нормально и ожидаемо, а не подмена.

Открытый код: другое устройство доверия, а не гарантия

Открытый исходный код — это когда исходный текст программы выложен и его может прочитать кто угодно, а не только сама компания-разработчик за закрытой дверью. Для человека, который сам никогда не откроет ни строчки этого кода — а это

подавляющее большинство пользователей, и это совершенно нормально, — открытость всё равно кое-что даёт, просто не то, что кажется на первый взгляд.

Это не гарантия, что программа безопасна: сама по себе открытость ничего не чинит и не проверяет автоматически. Это другое устройство доверия — то, что код в принципе может посмотреть кто угодно, а не только автор, означает, что подлость в нём держится хуже: рано или поздно её заметит кто-то из тех независимых людей, которые время от времени всё-таки читают чужой код — энтузиасты, исследователи безопасности, конкуренты. У закрытой программы такой массовой, никем специально не организованной проверки почти нет: код видят от силы автор и те немногие, кого он сам туда допустил, — например, аудитор по контракту, — а не любой желающий со стороны.

На практике это значит: при прочих равных стоит слегка предпочитать открытую программу закрытой, но не отказываться от закрытой только за то, что она закрытая. У открытости есть своя цена: реальная проверка требует, чтобы кто-то и правда потратил время и посмотрел, а это происходит не всегда и не сразу. (☒ почему открытый код помогает безопасности).

Контрольная сумма: сверяем две строки

У скачанного файла есть цифровой отпечаток — контрольная сумма, строка из букв и цифр, которая вычисляется по содержимому файла и меняется целиком, стоит поменять в файле хоть один байт. Издатель программы вычисляет эту сумму сам и публикует рядом со ссылкой на скачивание — обычно так и подписано: «SHA-256» и строка под ней. (☒ проверка подписи релиза). Ваша задача — вычислить ту же сумму у файла, который скачали именно вы, и сверить со строкой на сайте: они должны совпасть буква в букву. А если такой строки на сайте вообще нет — тоже ничего страшного: сумму публикуют далеко не все, для обычной программы это скорее редкость, чем правило, и в этом случае эта конкретная проверка просто не для неё — сверять там нечего.

Сначала используйте штатную проверку, без сторонней програм-

мы. На macOS выполните `shasum -a 256 путь-к-файлу`, на Linux — `sha256sum путь-к-файлу`, а в Windows — `certutil -hashfile путь-к-файлу SHA256`. Сравните результат с официальным значением: строки должны совпасть полностью. Если система показывает предупреждение Gatekeeper, не отключайте его и не выбирайте «Открыть в любом случае» просто для продолжения.

QuickHash-GUI — лишь необязательный вариант интерфейса: используйте его только из официального источника и после проверки подписи или хэша файла. Если Gatekeeper предупреждает о программе, сначала осознанно проверьте источник и подлинность; без такой проверки предупреждение не обходите.

Внутри у программы — вкладка `File` / `Файл`: сначала выбираете в списке алгоритм, тот же самый, что назван на сайте рядом со ссылкой (чаще всего это SHA-256, реже SHA-1 или MD5), затем сам скачанный файл — сумма считается автоматически. Выбор алгоритма — не мелочь: если в программе стоит один способ подсчёта, а издатель посчитал сумму другим, строки не совпадут даже у совершенно честного, ничем не повреждённого файла. Есть там же поле поле `Expected Hash Value` / `Ожидаемое значение хэша`: можно вставить в него строку с сайта, и программа сама сравнит две суммы.

Совпало — файл дошёл до вас именно таким, каким его выложил издатель: ни один байт не потерялся и не подменился по дороге. Не совпало хотя бы одним символом — файл лучше удалить и скачать заново, не открывая: даже одна несовпавшая буква означает, что перед вами не тот файл, который выложил издатель. (⊠ проверка контрольной суммы).

На телефоне устроено иначе, и в первую очередь это история Android: программы на нём куда чаще ставят не только из Google Play, но и файлом напрямую с сайта, а на iPhone почти всё идёт через App Store, и отдельно сверять сумму скачанного файла там обычно попросту негде — поставить программу в обход магазина у iPhone можно только в редких случаях. Для Android есть конкретное приложение — DeadHash: открытый исходный код (лицензия GPL-3.0), ставится из F-Droid, исходники лежат на GitHub. Считает

SHA-256, а заодно MD5, SHA-1, SHA-512 и другие. Последний релиз вышел в феврале 2025 года, а правки в исходном коде шли ещё в сентябре 2025-го. Такие маленькие утилиты, впрочем, меняются и забрасываются быстрее, чем что-либо ещё в этой теме, так что если DeadHash вдруг устареет, ищите замену по тем же двум признакам: дата последнего обновления в карточке приложения — если это было несколько лет назад, доверять не стоит, — и разрешения, которые приложение просит: простому калькулятору суммы файла ни к чему доступ к контактам, геолокации или чему-то ещё за пределами файлов на устройстве, и если он их просит, это повод поискать другое приложение.

Сумма подтверждает совпадение с тем, что выложил издатель, и больше ничего. Она не проверяет, что сам издатель заслуживает доверия и что программа внутри ведёт себя прилично, — если исходный файл на сайте уже был с сюрпризом, сумма это никак не покажет: она лишь подтвердит, что вы скачали именно тот файл с сюрпризом, а не какой-то другой. Сумма защищает от подмены по дороге, а не от нечестности источника.

Частичный ответ на вопрос о честности источника даёт VirusTotal — бесплатная публичная проверка файла или ссылки сразу десятками антивирусных движков. Предел на прямую загрузку файла — 32 МБ, но надёжнее всего вообще не загружать сам файл, а вставить в поиск его контрольную сумму — ту самую SHA-256, которую вы уже вычислили, — и посмотреть отчёт, если этот файл кто-то уже проверял до вас. Есть и честная оговорка: загруженные файлы попадают к партнёрам сервиса по безопасности и становятся доступны в платных инструментах для исследователей, так что конфиденциальный документ туда лучше не загружать, — а проверка по одной лишь сумме этого недостатка лишена. И вторая: несколько сработавших движков — это не приговор, а единичное срабатывание у малоизвестной программы часто оказывается ложным.

Сверять сумму у каждого скачанного файла никто не будет, и это нормально. Тратить на это время имеет смысл не всегда, а там, где программа ставится на основное устройство и надолго, а не там, где вы воспользуетесь ей один раз и забудете. (☒ как подойти к аудиту программы).

Видео: Tech Talk — Open Source: Does It Really Guarantee Data Security? https://www.youtube.com/watch?v=4UAevts1Qhg

Tech Talk — Open Source: Does It Really Guarantee Data Security? — подсказка к открытому коду, подписям и контрольным суммам; открытость сама по себе не гарантия.

- 4:34 — безопасность open source
- 6:19 — подпись релиза
- 7:00 — контрольная сумма
- 9:27 — аудит

☐ Сверить контрольную сумму у последнего файла, который вы скачали с сайта разработчика.

☐ Проверить в VirusTotal контрольную сумму программы, в источнике которой вы не до конца уверены.

Ревизия установленного: чистка холодильника, а не наведение порядка

Раз в какое-то время стоит открыть список установленных программ и пройтись по нему целиком — это ближе к чистке холодильника, чем к наведению порядка: там наверняка стоит что-то, что вы поставили один раз в 2019 году ради одного-единственного файла и с тех пор ни разу не открывали.

Каждую программу в списке стоит спросить об одном: пользовались ли вы ей за последний год хоть раз. Где на это посмотреть и как удалить программу — на каждой системе по-своему:

Windows: найти и удалить программу

1. «Пуск» ⊠ «Параметры» ⊠ «Приложения» ⊠ «Установленные приложения».
2. Дату последнего использования тут, увы, посмотреть негде — в Windows 11 такой возможности просто нет. Ближайшая подсказка — «Параметры» ⊠ «Система» ⊠ «Память» ⊠ «Рекомендации по очистке»: там есть отдельная категория неиспользуемых приложений, но как именно система решает, что счи-

тать неиспользуемым, Microsoft нигде не объясняет, так что это подсказка, а не точный ответ.
3. Рядом с нужной программой нажмите «Дополнительно» (кнопка с тремя точками) ⊠ «Удалить».
4. Если программы в списке нет или кнопка не срабатывает, тот же список можно найти иначе: Панель управления ⊠ «Программы» ⊠ «Программы и компоненты» — так снимаются некоторые программы, которых нет в новом интерфейсе «Параметров».

Официально: Удаление приложений и программ в Windows.

Mac: найти и удалить программу

1. Откройте Finder ⊠ папку «Программы» — это и есть список всех установленных программ.
2. Переключитесь на вид списком и через «Вид» ⊠ «Показать параметры вида» (⊠J) добавьте колонку с датой последнего открытия — по ней сразу видно, что вы не трогали год и больше.
3. Закройте программу, если она запущена. Если у неё есть собственный деинсталлятор — лучше воспользоваться им: по данным самой Apple, вместе с программой он убирает и её элементы входа, расширения и другие связанные данные.
4. Если отдельного деинсталлятора нет, перетащите программу из «Программы» в корзину, а потом очистите корзину через Finder.
5. Удаление программы не трогает документы и файлы, которые вы ею создавали, — это отдельно подтверждает сама Apple.

Официально: Удаление приложений на Mac.

iPhone: найти и удалить приложение

1. «Настройки» ⊠ «Основные» ⊠ «Хранилище iPhone».
2. Под названием каждого приложения там же показана дата последнего использования — а у тех, что вы вообще ни разу не открывали, стоит отдельная пометка об этом. Заодно видно, сколько места занимает каждое.
3. Откройте нужное приложение в списке и выбирайте одно из двух: «Выгрузить приложение» освобождает место, но

оставляет документы и данные на месте — значок остаётся, а при следующем нажатии приложение просто ставится заново; «Удалить приложение» убирает и само приложение, и все его данные.
4. Тот же список можно открыть и долгим нажатием на значок на экране, но точные подписи кнопок там неустойчивы — надёжнее идти через «Настройки», как выше.

Официально: Освобождение места в хранилище iPhone.

Android: найти и удалить приложение

1. «Настройки» ⊠ «Приложения» ⊠ «Все приложения» ⊠ выбрать приложение ⊠ «Удалить».
2. Отдельной даты последнего использования тут нет, но есть «Цифровое благополучие и родительский контроль» в настройках: на его панели по каждому приложению видно время использования и число запусков — по этим цифрам обычно сразу понятно, чем вы не пользовались.
3. На Android 15 и новее система умеет сама архивировать неиспользуемые приложения: «Настройки» ⊠ «Приложения» ⊠ нужное приложение ⊠ «Архивировать». Архивная копия освобождает место, но значок и данные остаются на месте, а само приложение возвращается одним нажатием.
4. Тот же список можно открыть и через магазин: Google Play ⊠ значок профиля ⊠ «Управление приложениями и устройством» ⊠ «Управление» ⊠ приложение ⊠ «Удалить».

Официально: Удаление приложений.

Если нет — удалить, не жалея; чаще всего программа так же легко ставится заново, если вдруг понадобится снова, — разве что для платной программы стоит перед этим убедиться, что лицензия или доступ к покупке никуда не делись, а совсем старую версию иногда у разработчика уже не найти. Логика простая: у каждой установленной программы есть доступ к части устройства, а значит, есть шанс, что именно в ней найдут уязвимость, которую никто больше не станет чинить, потому что автор давно забросил проект, а вы давно забыли, что она вообще стоит. Меньше программ — меньше таких дверей, вне зависимости от того,

насколько надёжной была каждая из них по отдельности.

Максимум

Ревизию можно провести ещё глубже — не только «пользуюсь или нет», а «что этой программе вообще нужно». У каждого приложения на телефоне есть список разрешений: доступ к контактам, камере, микрофону, геолокации, — и то, что приложение о чём-то попросило, вовсе не значит, что оно обязано это получить. Фонарику, например, не нужны ваши контакты и не нужна геолокация, сколько бы он их ни просил при установке: ему нужна ровно одна вещь — доступ к вспышке.

На Android посмотреть, кто что просит, можно тут: «Настройки» ⊠ «Безопасность и конфиденциальность» ⊠ «Конфиденциальность» ⊠ «Управление разрешениями». Список там устроен не по программам, а по видам доступа: отдельно все программы с доступом к камере, отдельно — к контактам, отдельно — к геолокации. На iPhone то же самое устроено иначе — Apple подробно описывает, как управлять доступом к информации в приложениях, в собственной инструкции. Стоит один раз пройтись по самым чувствительным пунктам — контакты, микрофон, геолокация, доступ ко всем файлам — и у каждого приложения в списке спросить себя, зачем ему это вообще нужно. Если ответа не находится, доступ можно забрать, не удаляя саму программу: почти всегда она продолжит работать как раньше, просто без лишнего.

- ☐ Пройтись по разрешениям приложений на телефоне и забрать доступ у тех, кому он явно не нужен.

Максимум

Есть и более радикальный инструмент — на случай, когда программу всё-таки хочется попробовать, а доверия к ней пока нет вообще никакого: песочница. Это отдельное, изолированное пространство на компьютере, внутри которого программа

запускается так, будто это единственное, что вообще существует на устройстве, — без доступа к вашим настоящим файлам, документам и остальным программам. Что бы программа ни делала внутри песочницы, за её пределы это не выходит; закрыли песочницу — и всё, что в ней происходило, исчезло вместе с ней.

В Windows, в редакциях Pro и выше, такая возможность встроена в саму систему — называется «Песочница Windows» и включается один раз в компонентах системы, а дальше открывается как обычная программа. На Mac прямого аналога с той же простотой нет, но есть настоящая замена — виртуальная машина: отдельная, полностью самостоятельная копия системы внутри окна. Вариантов несколько: UTM — открытый исходный код (лицензия Apache 2.0), бесплатна при загрузке с сайта и работает на Apple Silicon (та же программа продаётся в Mac App Store за $9.99 — это способ поддержать разработчика, а не другая версия); VMware Fusion — с 11 ноября 2024 года бесплатна для всех, включая коммерческое использование, но официальной поддержки у неё больше нет, только документация и сообщество; VirtualBox — версия 7.2.16 впервые даёт официальную стабильную сборку для Mac на Apple Silicon, раньше такая была только для Intel; и платный по подписке Parallels Desktop.

Ставить в такую машину придётся полноценную Windows, и вот тут кроется настоящая цена инструмента: по официальным требованиям самой Microsoft, Windows 11 нужно 64 ГБ места на диске, 4 ГБ памяти, два процессорных ядра, а для виртуальной машины отдельно нужны включённые Secure Boot и виртуальный TPM 2.0. На Mac с процессором Apple добавляется ещё одна сложность: нужна ARM-версия Windows, а её Microsoft не раздаёт так же свободно, как обычную. Это не пять минут и не одна кнопка, а отдельный проект на вечер — но именно он и есть настоящий ответ, когда программу очень нужно попробовать, а доверия к ней нет.

Получилось — когда из списка установленных программ пропали хотя бы три, которыми вы не пользовались весь последний год.

Если сводить тему к одной мысли: устройство защищает не только пароль и вовремя нажатая кнопка «обновить», но и то, что на него вообще пускают, — а это решение каждый раз принимаете именно вы, в момент клика «Скачать». Надёжные источники вместо одного случайного, честная сумма там, где это правда важно, и раз в год — ревизия списка программ: этого хватает, чтобы закрыть почти весь риск, который вообще берётся из установленного софта. Следующая тема — про второе пространство на Android: как держать под рукой приложения, которым не доверяешь до конца, но без которых не обойтись, не пуская их к остальному телефону.

Второе пространство на Android

Речь не о каждом читателе, а о конкретной ситуации: на телефоне есть приложение, которому вы не особенно доверяете, но всё равно им пользуетесь, — рабочее приложение с доступом к личной переписке, игра, которая просит контакты непонятно зачем, или программа, которая нужна раз в месяц, а тем не менее торчит в системе всё остальное время. Нет такого приложения — тема, скорее всего, не для вас, и остановиться можно прямо здесь, без малейшего чувства долга.

Сделай это прямо сейчас

- ☐ Поставить F-Droid — 5 минут
- ☐ Поставить из F-Droid приложение Shelter — 3 минуты
- ☐ Перенести в рабочий профиль одно приложение, которому не доверяете — 5 минут

Приложение, для которого остального телефона будто не существует

Android умеет то, что до включения редко приходит в голову: завести внутри одного телефона второе, полностью отдельное пространство. Это как отдельная сумка в прихожей для вещей, которым не вполне доверяете: пусть лежат под рукой, но не в шкафу с документами. Приложение внутри такого пространства не видит ваши обычные файлы, контакты, фотографии и остальные прило-

жения — для него их попросту не существует, будто это другой телефон, а не раздел на этом же. Если однажды такое приложение подведёт — утечкой, слежкой, обычной жадностью до разрешений, — оно унесёт с собой только то, что само туда и положило, а не содержимое всего телефона.

Максимум

Нужна стопроцентная разделяемость — возьмите второй телефон

Если для вашей ситуации важно, чтобы недоверенное приложение вообще не жило на том же устройстве, где находится личная переписка, второй Android-телефон — это 100% решение именно задачи разделяемости второго пространства: на нём отдельное устройство, отдельные приложения и отдельные данные, а не профиль внутри первого телефона.

SIM-карта или eSIM во втором телефоне не нужна. Подключите его к точке доступа первого телефона и пользуйтесь интернетом по Wi-Fi-раздаче. Мобильной связи на втором телефоне без SIM/eSIM не будет: звонки и SMS доступны только через интернет-приложения, если они вам подходят.

Ограничения существенные: раздача Wi-Fi с первого телефона не защищает первый телефон от его собственной компрометации, hotspot работает только пока первый аппарат рядом, включён и не разряжен, а второй телефон теряет интернет при отключении точки доступа. Поэтому это 100% решение для физического и системного разделения устройств, но не обещание абсолютной безопасности всей связки.

F-Droid: каталог, откуда всё это ставится

F-Droid — открытый каталог программ с открытым исходным кодом, независимый от Google Play: устанавливается он не из магазина, а прямо с сайта f-droid.org, и дальше спокойно живёт на те-

лефоне рядом с обычным магазином — один другому не мешает, это не замена, а второй, независимый источник программ. Именно оттуда, а не из Google Play, ставится и Shelter, о которой пойдёт речь дальше: магазин не пускает к себе программы, которые сами умеют устанавливать другие программы, а Shelter под эти правила не подходит — как и несколько похожих приложений, которых там тоже нет.

При установке файла с сайта Android почти наверняка покажет предупреждение — что-то вроде «Установка запрещена: разрешить для этого источника?» — это стандартная защита от случайной установки чего попало, а не сигнал, что с F-Droid что-то не так. На чистом Android разрешение включается здесь: Settings / Настройки ⊠ Apps / Приложения ⊠ Special app access / Специальный доступ ⊠ Install unknown apps / Установка неизвестных приложений ⊠ выбрать программу, которой скачивали файл, — браузер или файловый менеджер, — и включить Allow from this source / Разрешить установку из этого источника. На Samsung с One UI путь короче: Settings / Настройки ⊠ Security and privacy / Защита и конфиденциальность ⊠ More security settings / Другие настройки безопасности ⊠ Install unknown apps / Установка неизвестных приложений. После этого возвращаетесь и ставите F-Droid уже без вопросов. (⊠ установка F-Droid и Shelter).

Из него ставится не только Shelter — F-Droid вообще способ ставить программы с открытым кодом в обход магазина Google, а не запасной вариант на случай, когда программы нет больше нигде.

Получилось — когда F-Droid стоит на телефоне и открывается, а внутри — список программ, из которого можно ставить дальше.

Проверь себя. Как называется открытый каталог приложений, из которого ставят Shelter, — тот, из которого её ставят в обход магазина Google? Напишите название.

F-Droid. Это каталог, в котором лежат только программы с открытым исходным кодом: сам код виден всем желающим, а готовые файлы из него собирает сам каталог — значит, подделать что-то по дороге незаметно намного труднее, чем с обычным скачанным

файлом, который просто нужно принять на веру. Обратная сторона: приложений там заметно меньше, чем в обычном магазине.

Shelter: рабочий способ завести такое пространство

Технически это называется рабочий профиль — тот же механизм, которым Android и так умеет разводить личное и рабочее на корпоративных телефонах, обычно через учётную запись работодателя. Shelter даёт возможность завести такой профиль самому, без всякого работодателя: программа не изобретает ничего своего, а просто настраивает встроенный механизм системы для вас лично. Ни прав суперпользователя, ни перепрошивки — всё делается штатными средствами обычного Android-телефона.

Прежде чем ставить — важная оговорка, и лучше узнать её сейчас, а не после установки. У самого Android есть жёсткое ограничение: рабочий профиль на устройстве может быть только один, и это ограничение системы, а не прихоть Shelter. Если на телефоне уже есть рабочий профиль от работодателя — например, через корпоративное MDM-приложение, — настройка Shelter не сработает вовсе, не частично: программа честно показывает экран «Setup failed» с объяснением, что уже существующий рабочий профиль нужно удалить через системные настройки управления аккаунтами; название и путь зависят от версии Android. Обходного пути внутри самой Shelter для этого случая нет. Island и его сборка с открытым кодом Insular (о них — в блоке ниже) тоже не помогут: они используют тот же самый рабочий профиль и упираются в то же самое ограничение одного профиля на устройство.

Что делать, если это ваш случай: у телефонов на Android 15 и новее есть другой, отдельный тип изоляции — «Частное пространство» (Private Space, подробности и точный путь в настройках — в блоке ниже), и он умеет сосуществовать с рабочим профилем работодателя на одном телефоне. Есть и своя оговорка: на полностью корпоративных телефонах — тех, которыми владеет сам работодатель, а не на личном телефоне с рабочим профилем поверх, — «Частное пространство» тоже недоступно. И ещё одна: удалить рабочий про-

филь работодателя можно, но это решение с последствиями — вы теряете доступ к рабочим приложениям и данным, а разрешена ли такая самостоятельность вообще, зависит от политики самого работодателя.

Отдельная оговорка — для владельцев Xiaomi. Сам рабочий профиль Shelter на MIUI создать способна, а вот перенести в него сторонние программы — ради чего вся эта настройка вообще затевается — на MIUI не даёт сама прошивка: при попытке клонировать программу Shelter показывает отдельную ошибку о том, что перенос недоступен именно на MIUI. Так что прежде чем проходить всю настройку, разумнее сразу заглянуть в собственные средства прошивки — «Второе пространство» или «Клонирование приложений» в настройках (точные пути — тоже в блоке ниже).

Доверие к такой программе стоит не на слове, а на конкретных вещах: исходный код Shelter открыт на GitHub, и его может прочитать кто угодно — открытость сама по себе ничего не гарантирует, но вместе с этим сама программа не показывает рекламы и не тянет данные на сторонние серверы. Обновляется Shelter неспешно — в F-Droid последняя версия, 1.9.1, вышла в декабре 2023-го, — но это не то же самое, что заброшенность: правки в исходном коде продолжаются и в этом году, а сам проект описывает себя как программу в режиме поддержки, а не активной разработки — та же разница между зрелой программой и мёртвой, что и у QuickHash из темы про программы.

При первом запуске Shelter сама проводит через создание профиля — процесс занимает несколько минут, часть экранов в нём от самой системы, а не от Shelter. Вот как это выглядит по шагам:

Shelter: создание рабочего профиля (проверено в Shelter 1.9.1)

1. Поставьте Shelter из F-Droid — так же, как ставили сам F-Droid шагом раньше. Android может ещё раз спросить то же самое разрешение, на этот раз для самого F-Droid, а не для браузера, — путь к нему тот же, что описан в разделе про F-Droid выше.
2. Откройте Shelter. В проверенной версии 1.9.1 основные экраны были на английском; в других сборках язык и подписи могут отличаться. Первый экран — предупреждение с кнопка-

ми Continue / Продолжить и «Bye»: нажимайте Continue / Продолжить.

3. Дальше идут несколько вводных экранов подряд: Welcome to Shelter / Добро пожаловать в Shelter объясняет, что программа использует встроенный в Android рабочий профиль, A word on permissions / О разрешениях — зачем ей для этого роль управляющего профилем, Compatibility / Совместимость предупреждает, что на сильно переделанных прошивках системный механизм может повести себя иначе, чем на чистом Android. На каждом просто продолжаете дальше.
4. Последний экран перед стартом — Ready? / Готово?, за ним — Please wait... / Подождите...: система пытается создать рабочий профиль, это занимает несколько минут.
5. Здесь два исхода. Если на телефоне уже был рабочий профиль (см. оговорку выше) — почти наверняка появится Setup failed / Не удалось настроить, и дальше по этому пути не пройти. Если всё в порядке — вместо этого появится Action required / Требуется действие с просьбой открыть уведомление от Shelter.
6. Разверните шторку уведомлений и нажмите Click here to finish setting up Shelter / Нажмите здесь, чтобы завершить настройку Shelter. Отсюда управление перехватывает сама система Android, не Shelter, — дальше пойдут её собственные экраны.
7. Android попросит задать код разблокировки — PIN, графический ключ или пароль — отдельно для рабочего профиля: это стандартное требование системы, а не прихоть Shelter. Google-аккаунт на этом шаге не нужен, он понадобится только если вы захотите поставить в профиль Play Store.
8. В конце Android возвращает вас в Shelter с сообщением Shelter setup complete. Now restarting Shelter / Настройка Shelter завершена. Shelter перезапускается — программа перезапускается сама, и рабочий профиль готов.

Официально: исходный код Shelter на GitHub.

Получилось — когда Shelter стоит на телефоне, а при первом запус-

ке уже виден экран создания рабочего профиля.

Видео: Tech Talk — How to Isolate Apps on Android with Shelter: Complete Data Protection (2025) https://www.youtube.com/watch?v=DX8QAqKDi8Y

Tech Talk — How to Isolate Apps on Android with Shelter: Complete Data Protection (2025) — подсказка к установке F-Droid и Shelter, клонированию и настройкам профиля; названия меню зависят от Android и оболочки.

- 1:47 — установка F-Droid и Shelter
- 3:16 — клонирование
- 5:00 — изоляция
- 7:25 — настройки

Максимум

Shelter — не единственный вход в эту дверь, а в некоторых случаях (см. оговорки выше) — и вовсе не рабочий. На чистом Android 15 и новее похожая изоляция есть прямо в системе, под именем «Частное пространство» (Private Space): Настройки ⊠ Защита и конфиденциальность ⊠ Частное пространство. Разблокированное, оно видно отдельным разделом внизу списка программ; заблокированное — приложения внутри пропадают из списка целиком, будто их и не ставили. Google-аккаунт для него не обязателен, хотя сам Google советует завести под это дело отдельный.

У Samsung похожая изоляция называется «Защищённая папка» (Secure Folder): Настройки ⊠ Защита и конфиденциальность (на части прошивок раздел подписан «Биометрия и безопасность») ⊠ Другие настройки безопасности ⊠ Защищённая папка. Условие, о котором стоит знать заранее, — для неё обязателен аккаунт Samsung.

У Xiaomi на HyperOS/MIUI есть «Второе пространство»: Настройки ⊠ Второе пространство (на части прошивок — на шаг глубже: Настройки ⊠ Расширенные настройки ⊠ Второе пространство). Честная оговорка: на части новых сборок HyperOS

его находят не всегда — не по объявленному решению Xiaomi, просто пропадает или ведёт себя нестабильно на отдельных моделях. Ближе к тому, что делает Shelter, — отдельный пункт «Клонирование приложений» (Настройки ⊠ Клонирование приложений): именно он, а не «Второе пространство», стоит открыть, если родная Shelter на MIUI отказалась клонировать программы (см. оговорку выше).

Если на вашем телефоне уже есть что-то из этого списка, разумнее сперва заглянуть туда: встроенное решение поддерживает сам производитель или сам Android, и ставить поверх него ещё одну программу незачем. Есть и сторонние приложения с похожей идеей — например, Island, — но в F-Droid самого Island нет: там лежит Insular, форк Island с вырезанными компонентами Google. Устроены они технически так же, как Shelter, — тот же рабочий профиль, — а значит, упираются в то же самое ограничение одного профиля на устройство. Выбор между всеми этими вариантами — дело вкуса, версии Android и конкретного телефона, а не принципа.

Что стоит унести во второй профиль

Кандидатов на переезд обычно немного, но они узнаваемы. Приложение, которое просит контакты, микрофон и геолокацию ради одной скромной функции — сканера документов, конвертера файлов, простого редактора фото, — классика: столько разрешений ему на самом деле не нужно, а раз оно всё равно просит, разумнее держать его там, где смотреть попросту не на что. Рабочее приложение от работодателя — тоже частый гость: у него своя политика безопасности и свои требования к устройству, а вы бы предпочли, чтобы оно не видело остальной телефон. И третий вид — то, чем вы пользуетесь раз в месяц: приложение доставки, которым открываете дверь подъезда, программа ради одной конкретной справки, — вещь нужная, но не настолько, чтобы она постоянно висела рядом с личной перепиской.

Механически перенос выглядит просто: открываете Shelter, на главном экране находите нужное приложение в общем списке

и нажимаете на его название — появится окошко с вариантами, один из которых клонирует программу в рабочий профиль (в английском интерфейсе он подписан `Clone to Shelter` / `Клонировать в Shelter`, по-русски — что-то вроде «Клонировать»). В первый раз Shelter, скорее всего, попросит то же самое разрешение на установку, которое вы уже включали для F-Droid, — тот же самый переключатель «Установка неизвестных приложений», путь к нему описан в разделе про F-Droid выше, только на этот раз для самой Shelter. После этого на телефоне появляется вторая, изолированная копия приложения — оригинал никуда не девается, а какой из двух копий пользоваться дальше, решаете сами. (☒ клонирование приложения).

Получилось — когда рядом с обычной иконкой приложения появилась вторая, с пометкой рабочего профиля, а какой из двух копий пользоваться дальше, вы уже решили сами.

Максимум

Тот же механизм неплохо работает и без всякой угрозы — просто как способ развести рабочее и личное по разным углам. Рабочую почту, корпоративный мессенджер, таск-трекер можно держать в отдельном профиле не потому, что вы кому-то не доверяете, а потому что так удобнее: вечером и в отпуске рабочий профиль можно поставить на паузу одной кнопкой, и рабочие уведомления попросту перестанут приходить — вместо того чтобы полагаться на силу воли не открывать почту. Это уже не столько про безопасность, сколько про голову: меньше рабочего на виду в нерабочее время — меньше поводов туда заглянуть «на минутку». Личный профиль от этого тоже выигрывает: рабочие иконки, звуки и бейджи не мешаются среди личных весь день, а не только тогда, когда вы сами вспомнили их спрятать.

Как это выглядит в быту

После настройки телефон не превращается в нечто незнакомое — иконки рабочих копий выглядят так же, как обычные, только с маленькой пометкой в углу, которая и отличает рабочую копию от личной. На части лаунчеров, в том числе на чистом Android, рабочие приложения при этом собираются в отдельную вкладку «Работа» в общем списке программ — это уже ближе к отдельному разделу, чем к незаметной метке, и первое время может немного сбивать с толку, если вы её не ждали. Открывается такое приложение точно так же, одним касанием, — разница только в том, что происходит внутри. У всего профиля целиком есть один переключатель — «Пауза» или похожий пункт рядом со списком приложений рабочего профиля, — и одним касанием весь профиль замирает разом: ни одно приложение внутри него не работает в фоне, не шлёт уведомлений и не расходует интернет и батарею, пока вы сами не включите профиль обратно. (☒ настройки рабочего профиля).

Максимум

Пауза выключает всё сразу, а есть и более точечный инструмент — заморозка одного конкретного приложения внутри профиля. Замороженное приложение никуда не девается: значок остаётся на месте, само оно установлено, но не запускается само, не проверяет обновления и не шлёт уведомления, пока вы вручную его не разморозите. Смысл тот же, что и у паузы всего профиля, только в масштабе одной программы: приложение доставки или разовая справка, которой вы пользуетесь раз в месяц, девять дней из десяти может просто лежать замороженным, ничего не делая и никого не слушая, и оживать только на те пять минут, когда действительно нужна.

- ☐ Заморозить в рабочем профиле приложение, которое нужно раз в месяц.

Цена вопроса — и почему она реальная

Изоляция здесь не абсолютная — это плотная перегородка, а не бетонная стена. Часть приложений умеет распознавать, что её запустили в рабочем профиле, а не в обычном, и просто отказывается работать: так ведут себя некоторые банковские и государственные приложения — это их собственное решение, а не ограничение Android, и обойти его не получится, разве что оставить такое приложение там, где оно и было, — в личном профиле.

Есть цена и у самого переноса, отдельно от привычки переключаться. Клон — это не копия данных, а свежая, пустая установка: в неё придётся заново войти во все нужные учётные записи, и увидеть данные из личной копии она не сможет при всём желании — в этом весь смысл разделения, но и вся его цена. Обновляются такие клоны тоже не сами по себе: Shelter не магазин приложений и не следит за версиями внутри профиля — обновлять их приходится тем же способом, каким они туда попали, поставив F-Droid (а если нужно — и Play Store) уже внутри самого профиля и обновляясь оттуда, как с отдельного телефона.

Удаление профиля — решение без черновика. Android перед этим честно предупреждает: «Удалить рабочий профиль?» — и поясняет дальше: «Все приложения и данные, находящиеся в этом профиле, будут удалены» — и делает ровно то, что обещает, без корзины и отмены. Если однажды захочется убрать саму Shelter, порядок важен: сначала удаляется рабочий профиль, через «Настройки» ⊠ «Аккаунты», и только потом — программа Shelter; в обратном порядке система рискует не дать корректно снять профиль.

Первое время путают и уведомления: два похожих значка одного и того же мессенджера в списке, система, которая переспрашивает, каким профилем открыть ссылку, — переключение между профилями входит в привычку не сразу. Пока профиль активен, уведомления в нём приходят как обычно — но у приложений, завязанных на сервисы Google, для этого должны быть установлены сами Google Play Services внутри профиля, отдельно от личной копии, иначе присылать их попросту нечему.

Есть и оговорка отдельно про сам путь установки — тот, кото-

рым на телефон попадают и F-Droid, и Shelter. Google требует, чтобы приложения на сертифицированных Android-устройствах приходили от разработчика с подтверждённой личностью — независимо от того, ставится программа из магазина или в обход него. Регистрация открылась для всех разработчиков в марте 2026-го, а первое реальное применение правила стартует 30 сентября 2026-го — и пока только в четырёх странах: Бразилии, Индонезии, Сингапуре и Таиланде. Глобальный запуск Google анонсировала на 2027 год, но точную дату и механизм ещё не назвала. Для тех, кто всё же захочет поставить неподтверждённое приложение, предусмотрен нарочито неудобный обходной путь — включить режим разработчика, перезагрузить телефон, подождать 24 часа, заново подтвердить личность и несколько раз согласиться; он заработал по всему миру в августе 2026-го. Есть и бесплатная регистрация «для ограниченного распространения», но она рассчитана всего на 20 устройств — сам F-Droid ещё в феврале 2026-го публично выступил против этих правил, назвав их угрозой для себя: каталог распространяет программы от множества псевдонимных авторов, которые не станут называть Google свою настоящую личность, а лимит в 20 устройств делает бесплатный уровень бесполезным для публичного каталога. Что это значит для вас прямо сейчас: F-Droid и Shelter сегодня ставятся совершенно нормально, и 30 сентября это не изменится нигде, кроме тех четырёх стран. А что будет в 2027-м — прогноз по объявленным правилам, а не свершившийся факт, и если однажды путь и правда усложнится, вашей вины в этом не будет.

Это самая дорогая по усилиям тема бюллетеня, и она правда не для всех — здесь есть что настраивать и к чему привыкать, а не одна кнопка на пять минут.

Если сводить тему к одной мысли: второе пространство окупает потраченное время только при одном условии — когда на телефоне и правда завелось то самое приложение, которому не хочется доверять остальной телефон целиком. Нет такого приложения — и тема попросту не понадобится, без всякой драмы по этому поводу. Девять тем про риск в бюллетене на этом заканчиваются — обязательная часть позади. Дальше идёт одна-единственная тема вне очереди, «Основы работы с нейросетями»: она другая по сути — не

про то, как ничего не потерять, а про то, как кое-чему научиться, — так что относиться к ней стоит соответственно, без спешки и без ощущения долга.

Основы работы с нейросетями

Эта тема не про то, что вы рискуете потерять, а про то, чему стоит научиться, — потому и стоит вне очереди.

Сделай это прямо сейчас

- ☐ Открыть один из трёх сервисов и задать ему свой настоящий вопрос — 5 минут
- ☐ Переспросить то же самое: попросить короче, проще или списком — 3 минуты
- ☐ Проверить в ответе один факт, который важно не переврать — 5 минут

Что такое чат-бот на самом деле

Проще всего представить его не поисковиком со справочником, а очень начитанным приятелем, который предсказывает продолжение текста. Он не «ищет ответ» в базе данных, а на лету угадывает, какое слово должно идти дальше, — угадывает при этом очень хорошо, потому что прочитал огромное количество текста, но именно угадывает, а не сверяется со списком фактов.

Отсюда прямое и не самое удобное следствие: такой приятель умеет **уверенно ошибаться**. Внутри у него нет пометки «это я знаю точно, а это подставил по догадке» — точный факт и чистая выдумка рождаются одним и тем же способом угадывания следующего

слова, поэтому и звучат одинаково гладко. По одному тону ответа отличить одно от другого попросту нельзя.

Как спросить, чтобы вышел толк

Хороший запрос — конкретный, с контекстом и с указанием, какой формат и объём нужны на выходе. Чем меньше вы оставили на догадки, тем меньше придётся переделывать: модель не умеет читать мысли и достраивает недостающее по среднему, а не по тому, что вы на самом деле имели в виду.

Чаще всего первый ответ выходит посредственным именно поэтому: вопрос был общим, и достраивать пришлось слишком многое. Дело не в том, что вы плохо спрашиваете: с первого раза почти никто не формулирует всё, что нужно, и даже подробный запрос обычно доводят за круг-другой. Относиться к первому ответу как к черновику — нормальный первый заход, а не сбой и не повод считать себя неспособным разобраться. Переспросить не стыдно: весь навык в этом и состоит.

Выглядит это буднично. Спросили `Как оформить налоговый вычет за лечение` — и получили две страницы сплошного текста с терминами. Вторым сообщением не начинают заново, а чинят ровно то, что не устроило: `Слишком длинно и много терминов. Перепиши списком из семи шагов, простыми словами, без канцелярита: что делать по порядку.` Тот же диалог, тот же вопрос, но ответ приходит уже в нужном виде — семь шагов, которые останется сверить с сайтом налоговой. Формула короткая: сказать, что не так с прошлым ответом, и сказать, каким он должен быть вместо этого.

Получилось — когда вы переспросили тот же вопрос ещё раз: попросили короче, проще или списком — и ответ на глазах стал другим.

Проверь себя. Нужно письмо в управляющую компанию про текущий стояк. Какой запрос вернёт текст, который можно отправлять почти как есть?

1. `Напиши письмо`

2. `Напиши письмо в управляющую компанию, чтобы они наконец что-нибудь сделали`
3. `Напиши вежливое письмо в управляющую компанию: в ванной вторую неделю течёт стояк, две заявки по телефону остались без ответа. Официальный тон, д о десяти строк, с просьбой прислать мастера на э той неделе.`

Третий. Разница не в длине, а в том, что в нём есть ровно то, чего модель знать не может: что случилось, что уже пробовали, каким тоном и какого объёма нужен результат. Первые два она тоже выполнит — и вернёт усреднённое письмо ни о чём, которое придётся переписывать целиком. Правило простое: чем меньше вы оставили на догадки, тем меньше придётся переделывать. И да, третий запрос дольше писать, чем первый, — но короче, чем потом переписывать ответ.

Один и тот же цикл на любом сервисе

Спросил своими словами — прочитал — переспросил, если непонятно или неверно, — это весь цикл целиком, и он не зависит от того, каким сервисом пользоваться. Три сервиса, где его можно попробовать прямо сейчас, — и внутрь каждый пускает по-своему.

ChatGPT пускает вообще без аккаунта: на странице есть вариант остаться неавторизованным, и можно просто написать вопрос в поле. Плата за это — разговор всего один, самая сильная модель отвечает ограниченное число раз, а дальше подхватывает модель попроще, и ничего не сохраняется у вас: почистили куки или зашли с другого устройства — переписки нет. Из России он обычно не открывается без VPN; если так — просто идите к следующему сервису, цикл везде одинаковый.

DeepSeek без аккаунта не пускает, но регистрация занимает меньше минуты: почта или вход через Google. Номер телефона там принимают только китайский, так что этот путь мимо нас.

Grok тоже просит аккаунт и принимает на выбор почту, Google или аккаунт X (бывший Twitter). Именно на выбор: когда-то Grok дей-

ствительно открывался только через X, и многие так это и запомнили, — но заводить X ради него сегодня не нужно.

Там, где просят почту, не обязательно светить основной ящик: под такие регистрации удобно завести отдельный, которым не жалко расплачиваться за спам, — подробнее этот приём разобран в теме про приватность. А дальше в каждом сервисе — то же самое поле для вопроса и та же самая привычка переспрашивать.

Про то, что в чат-бот не отправляют — паспорт, рабочие документы, чужие переписки, — сказано в теме про безопасность при использовании ИИ.

Получилось — когда в одном из трёх сервисов открыт диалог, а в нём лежит ответ на ваш настоящий, а не тестовый вопрос.

Что бесплатные версии дают на бытовых задачах

На повседневных делах бесплатных веб-версий этих трёх сервисов обычно хватает с запасом: набросать и вычитать текст, объяснить что-то простыми словами, накидать вариантов, перевести, помочь с несложным кодом, пересказать длинный текст коротко. Ровно то, чем и стоит начинать пользоваться, прежде чем разбираться в чём-то более серьёзном.

> **Максимум**
>
> Приёмы посерьёзнее, когда простого вопроса уже мало. Дать модели роль — «побудь редактором этого письма», «побудь моим корректором» — и ответ станет заметно ближе к нужному тону, чем на голый вопрос без роли. Показать пример нужного результата, а не только описать его словами: одна строка «вот примерно в таком духе» экономит несколько кругов переспрашивания. Попросить рассуждать по шагам, если задача хоть немного сложная, — так виднее, где именно рассуждение свернуло не туда. И главное — доводить итерациями, а не соглашаться с первым черновиком: это то же самое переспрашивание из базового цикла, только более осознанное.

Максимум

Три названных сервиса не одинаковы, и разница у них вполне конкретная. ChatGPT — самый универсальный: поиск по интернету и генерация картинок работают уже в бесплатной версии, есть голосовой режим, и он одинаково уверенно держится и в разговоре, и в коде; главный минус для нас в том, что из России он без VPN обычно не открывается. У DeepSeek есть то, чего нет ни у одного из двух других: веса модели выложены открыто, под лицензией MIT, — то есть её в принципе можно запустить у себя на компьютере, без чужих серверов в цепочке; тот самый локальный вариант из темы про безопасность при использовании ИИ. А ещё у его чата вообще нет платной подписки, так что и предлагать её вам никто не будет. Grok единственный подключён к живой ленте X: он видит свежие посты и то, что там сейчас обсуждают, умеет искать по интернету и по X сразу (режим DeepSearch), а картинки умеет не он один, зато видео — только он.

А вот с лимитами бесплатных тарифов честный ответ такой: назвать вам цифру значило бы соврать. Они меняются, и источники расходятся между собой даже в том, какая модель сегодня отвечает бесплатным пользователям. Обещать, что там прямо написана ваша цифра, тоже не буду — компании меняют это без предупреждения; адреса обеих страниц — ниже, в «Честных ограничениях». У DeepSeek сравнивать нечего: платного тарифа у чата нет, есть только бесплатный.

Никто не обязывает выбирать один раз и навсегда: попробовать один и тот же вопрос в разных сервисах — законный способ понять, какой удобнее лично вам, а не признак нерешительности.

Честные ограничения

У самой модели есть дата, после которой она по памяти ничего не знает, — но сервис умеет ходить в интернет и искать, так что спрашивать про недавнее можно, просто к найденному стоит относить-

ся с той же проверкой, что и к любому другому ответу. Модель к тому же способна на уверенные выдумки: заявляет несуществующий факт или источник тем же ровным уверенным тоном, что и правду, — для этого явления даже есть отдельное слово, «галлюцинации», и означает оно именно это: ответ звучит убедительно, а проверки не выдерживает. У бесплатного тарифа есть свои лимиты — по числу сообщений или по их частоте, и у каждого сервиса свои; конкретные цифры то и дело меняются, так что смотреть их стоит только на странице тарифов самого сервиса, а не в чьём-то пересказе: у ChatGPT это openai.com/chatgpt/pricing, у Grok — x.ai/pricing. Но и там цифра не высечена в камне — это просто единственное место, где её вообще стоит искать. У DeepSeek искать негде: платного тарифа у его чата попросту нет. Видит ли новый разговор то, что вы обсуждали раньше, зависит от сервиса и настроек аккаунта и бывает по умолчанию по-разному; а вот что не зависит от этой настройки совсем — то, что вы уже отправили, всё равно остаётся на серверах компании независимо от того, включена «память» или нет.

Простая защита от уверенных выдумок — выбрать в уже полученном ответе один факт, который важно не переврать: дату, цифру, имя, — и свериться с ним отдельно, а не поверить на слово только потому, что звучало гладко. Сверяться проще всего так: вбить этот факт в обычный поисковик и найти хотя бы два источника, независимых друг от друга и сходящихся в одном, — два пересказа одной и той же новости за два источника не считаются. А если факт официальный — срок, тариф, норма закона, — идти сразу к первоисточнику: на сайт самого ведомства или в текст закона, а не к тому, кто его цитирует. Есть и третий путь, совсем быстрый: задать тот же вопрос второму сервису из трёх и посмотреть, сойдутся ли ответы: разошлись — точно надо проверять, сошлись — доверия больше, но и это ещё не доказательство. Подробнее — в «максимуме» ниже.

Получилось — когда вы нашли в ответе такой факт и проверили его отдельно, а не приняли на веру просто потому, что тон был уверенным.

Максимум

Сверка важного ответа со вторым сервисом — самый дешёвый способ поймать уверенную выдумку. Если от ответа зависит что-то реальное — деньги, здоровье, документ, — задать тот же вопрос второму сервису из трёх и сравнить ответы занимает пару минут, а расхождение сразу видно: если оба сходятся, доверия больше, если расходятся — самое время проверить факт отдельно, а не верить на слово ни одному из двух.

- ☐ Задать один и тот же важный вопрос двум сервисам из трёх и сравнить ответы.

Если сводить тему к одной мысли: это очень начитанный приятель, который прочитал полбиблиотеки и физически не умеет сказать «не знаю», — спрашивать у него полезно, а вот верить на слово в вопросах денег и здоровья не стоит. Первый ответ редко выходит таким, как надо: чаще всего просто потому, что вопрос был общим. Переспросить тут не признание неудачи, а единственный рабочий способ довести дело до толку.

На этом бюллетень заканчивается — девять тем про риск и один бонус, готово. Всё, что нужно сделать, собрано в одном месте: в книге это последняя глава, на сайте — счётчик на главной, который считает то же самое. Возвращаться к невыполненным пунктам можно когда угодно и в любом порядке: спешки тут никакой не было и нет.

Чек-лист: всё, что нужно сделать

- ☐ Скачать KeePassXC с keepassxc.org — 3 минуты
- ☐ Создать базу и придумать мастер-пароль — 7 минут
- ☐ Сменить пароль на почте и сохранить новый в базу — 5 минут
- ☐ Удалить старый пароль из последней переписки — 3 минуты
- ☐ Перенести в базу ещё один старый сайт, который вспомнится первым — 5 минут
- ☐ При создании новой базы настроить время расшифровки в мастере защиты до завершения создания базы; KDF в расширенных настройках не менять.
- ☐ Положить копию базы на второе устройство и убедиться, что она там открывается.
- ☐ Завести общую базу KeePassXC с близким человеком для паролей, которые нужны вам обоим, — например для администратора домашнего роутера.
- ☐ Поставить на телефон приложение-генератор кодов — 3 минуты
- ☐ Включить второй фактор на почте — 6 минут
- ☐ Включить «Облачный пароль» в Telegram — 4 минуты
- ☐ Включить двухшаговую проверку в WhatsApp — 3 минуты
- ☐ Сохранить резервные коды от почты в базу паролей — 3 минуты
- ☐ Посмотреть в настройках безопасности почты, поддерживает ли она аппаратный ключ.
- ☐ Включить автообновление на телефоне — 3 минуты
- ☐ Поставить обновление, которое телефон откладывает уже ме-

сяц — 2 минуты
- ☐ Включить автообновление на компьютере и в браузере — 5 минут
- ☐ Открыть официальную страницу поддержки своей модели телефона и проверить, до какого года ей обещаны обновления.
- ☐ Зайти в настройки роутера, проверить обновление прошивки и заодно сменить заводской пароль администратора.
- ☐ Положить банк и почту в закладки и заходить только оттуда — 3 минуты
- ☐ Записать в контакты телефон банка с обратной стороны карты — 2 минуты
- ☐ Найти в почте последнее письмо «подтвердите данные» и рассмотреть адрес отправителя — 5 минут
- ☐ Открыть сайт своего банка, нажать на замочек и посмотреть, кому и кем выдан сертификат.
- ☐ На публичном Wi-Fi войти в банк или почту не через сеть, а переключившись на мобильный интернет.
- ☐ Проверить, включено ли на телефоне облачное резервное копирование — 5 минут
- ☐ Включить на компьютере автоматическое копирование на внешний диск — 5 минут
- ☐ Скопировать базу паролей куда-нибудь ещё, кроме компьютера — 5 минут
- ☐ Найти, где лежат ваши фотографии, и убедиться, что они не только в телефоне — 5 минут
- ☐ Достать из резервной копии один файл и открыть его — убедиться, что копия действительно рабочая.
- ☐ Договориться с близкими о контрольном слове — 5 минут
- ☐ Условиться дома: деньги — только после обратного звонка на известный номер — 2 минуты
- ☐ Пролистать историю переписки с чат-ботом и удалить оттуда личные данные — 5 минут
- ☐ Найти в настройках чат-бота пункт про обучение на ваших переписках и выключить его.
- ☐ Поставить в браузер блокировщик рекламы и трекеров — 3 минуты
- ☐ Выбрать защищённый мессенджер и написать в нём одному человеку — 5 минут

- ☐ Открыть свою страницу в соцсети от чужого имени и посмотреть, что видно — 7 минут
- ☐ Завести отдельный почтовый адрес под регистрации в магазинах и рассылки.
- ☐ Удалить MAX с телефона (не удаляется — отключить), а если без него не обойтись — перенести его в отдельный рабочий профиль.
- ☐ Создать аккаунт в Signal или Session, сохранить секрет восстановления вне чата и проверить одного собеседника через второй канал.
- ☐ Проверить, откуда скачана программа, которой пользуетесь чаще всего — 3 минуты
- ☐ Открыть список установленных программ и удалить три, которыми не пользуетесь — 10 минут
- ☐ Сверить контрольную сумму у последнего файла, который вы скачали с сайта разработчика.
- ☐ Проверить в VirusTotal контрольную сумму программы, в источнике которой вы не до конца уверены.
- ☐ Пройтись по разрешениям приложений на телефоне и забрать доступ у тех, кому он явно не нужен.
- ☐ Поставить F-Droid — 5 минут
- ☐ Поставить из F-Droid приложение Shelter — 3 минуты
- ☐ Перенести в рабочий профиль одно приложение, которому не доверяете — 5 минут
- ☐ Заморозить в рабочем профиле приложение, которое нужно раз в месяц.
- ☐ Открыть один из трёх сервисов и задать ему свой настоящий вопрос — 5 минут
- ☐ Переспросить то же самое: попросить короче, проще или списком — 3 минуты
- ☐ Проверить в ответе один факт, который важно не переврать — 5 минут
- ☐ Задать один и тот же важный вопрос двум сервисам из трёх и сравнить ответы.