Техника цифровой безопасности

2026

Содержание

Красный список **4**

Прежде чем начать **11**

Пароли и менеджер паролей **12**
Зачем не один пароль 12
Поставить менеджер паролей 13
Создать базу и мастер-пароль 16
Придумать пароль для сайта 26
Подключить расширение браузера 30
Записать новый сайт 34
Начать перенос с почты 36
Сохранить базу 37
Открыть базу на телефоне 38
Перенести остальные сайты 41
Удалить пароль из переписки 42
Передать пароль человеку 42

Двухфакторная аутентификация **49**
Установить приложение для кодов 50
Включить 2FA в почте 58
Включить 2FA в Telegram 60
Включить 2FA в WhatsApp 62
Сохранить резервные коды 63

Обновления ОС и приложений **66**
Почему нельзя откладывать обновления 66

Какие дыры уже известны 67
Включить автообновление на телефоне 69
Включить автообновление на компьютере 71
Установить отложенное обновление 75
Понять, что устройство пора менять 76

Фишинг, поддельные сайты и сертификаты **80**
Как работает обман 80
Раскрыть ссылку до клика 82
Прочитать адрес сайта 83
Заметить подмену в адресе 86
Что значит замочек в браузере 87
Заходить в банк и почту своим путём 89
Проверить странное сообщение от знакомого 90
Позвонить по известному номеру 91
Что делать после ввода пароля 93

Резервные копии **97**
Сделать три копии на двух носителях 97
Проверить резервную копию телефона 99
Настроить копирование на внешний диск 105
Скопировать базу паролей в резерв 110
Сохранить фото и важные файлы 112
Зачем нужны копии 115

Безопасность при использовании ИИ **117**
Проверить звонок обратным звонком 117
Договориться о контрольном слове 119
Убрать лишнее из запроса чат-боту 120
Проверить ответы чат-бота 124

Приватность в сети **128**
Поставить блокировщик рекламы 128
Сменить поисковик по умолчанию 131
Выбрать защищённую связь 134
Проверить страницу в соцсети 140
Включить VPN 142
Подключаться к публичному Wi-Fi 144

Выбор и проверка программ **147**
Выбрать, откуда скачать программу 147
Распознать ловушку «скачать бесплатно» 151
Оценить открытый код 152
Сверить контрольную сумму 153
Проверить установленные программы 157

Второе пространство на Android **165**
Зачем второе пространство на телефоне 166
Поставить F-Droid 166
Завести пространство в Shelter 168
Перенести приложения во второй профиль 173
Пользоваться вторым пространством 175
Какие у второго пространства ограничения 177

Основы работы с нейросетями **180**
Что такое чат-бот 180
Попробовать чат-бот в сервисе 181
Задать вопрос боту 183
Что умеют бесплатные версии 185
Проверить ответы бота 187

Чек-лист: всё, что нужно сделать **189**

Красный список

Если вы только начинаете, начните отсюда. Здесь десять правил, которые закрывают самые частые сценарии. Они расположены по важности, по мнению авторов. Каждое правило — это одно конкретное действие по шагам; если в какой-то строке сказано «выберите», выбор уже сделан за вас. Никакой спешки: можно делать по одному правилу в день.

1. **Никому не называйте коды из СМС и приложений.** Ни «сотруднику банка», ни «службе безопасности», ни «курьеру». Настоящий банк кода не спрашивает никогда: код нужен, чтобы войти в ваш счёт, а не чтобы его «спасти». Попросили код — положите трубку и перейдите к правилу 2.

2. **Бросьте трубку и перезвоните сами.** Позвонили «из банка» или «из полиции» и торопят? Если звонок настоящий, банк это подтвердит.

    1. Заранее найдите на своей банковской карте телефон банка и запишите его в контакты под именем «Банк».
    2. Позвонили «из банка» — положите трубку.
    3. Откройте контакт «Банк» и позвоните сами. Результат: вы говорите с настоящим банком, а не с тем, кто позвонил вам.

    Если номера на карте нет, берите его из договора с банком. *(вывод автора)* Подробнее.

3. **Не переходите по ссылкам из сообщений, особенно неожиданных.** Поддельный сайт похож на настоящий, а

закладка ведёт на тот адрес, который вы сохранили. Зайти в банк или на сайт госсервисов лучше через свою закладку в браузере либо через приложение банка. Закладку делают один раз.

1. Наберите адрес банка в адресной строке браузера вручную. Адрес возьмите из договора с банком или из его приложения, а не из поиска и не из сообщения. *(вывод автора)*
2. Нажмите `Ctrl+D` на Windows или `Cmd+D` на Mac[1] и подтвердите сохранение в открывшемся окне.
3. Проверьте: закройте вкладку и откройте банк из списка закладок браузера. Результат: открывается тот же сайт, который вы набрали вручную.

Заходите в банк только так: из закладки или из приложения банка, а не по ссылке из сообщения. Подробнее.

4. **Договоритесь с близкими о «контрольном слове».** Мошенники умеют подделывать голос по короткой записи.[2] Если «внук» просит срочно перевести деньги, спросите слово, которого посторонним знать неоткуда.

    1. Придумайте с близкими фразу из двух-трёх случайных слов, не связанных с вами. Не берите имя питомца и фамилию из соцсетей: их легко найти. *(вывод автора)*
    2. Не пишите слово в переписке и не говорите его в голосовых сообщениях.
    3. На просьбу о деньгах спросите слово. Чем бы ни ответил собеседник, положите трубку и перезвоните этому человеку на номер, который вы знали заранее.

    Если собеседник путает слово или торопит — сразу кладите трубку и перезванивайте сами: слово не заменяет обратный звонок. Подробнее.

---

[1] Справка Chrome: комбинации клавиш, «сохранить страницу как закладку»: `Ctrl + d` на Windows, ⌘ + d на Mac, на англ. Подпись кнопки подтверждения в окне закладки не проверялась. Проверено: 2026-10-13.

[2] FTC: Scammers use AI to enhance their family emergency schemes, на англ. Проверено: 2026-10-13.

5. **Заведите менеджер паролей.** Это программа, которая сама помнит пароли от всех сайтов, а вам нужно помнить один главный. Так на каждом сайте будет свой пароль, и утечка в одном месте не откроет остальные.[3] Берите KeePassXC: у него открытый код, и он бесплатный. *(вывод автора)*

    1. Откройте keepassxc.org/download и нажмите `Download for Windows` или `Download for macOS`.[4]
    2. Запустите скачанный файл и следуйте шагам установщика.
    3. Создайте базу. В окне «Доступ к базе данных» наберите придуманную фразу: из нескольких слов, которые раньше не встречались вместе, длиннее 20 символов, не цитата и не личные данные; повторите её в поле подтверждения. Условия и пример разобраны в теме «Пароли». Не хотите придумывать сами — нажмите значок кубика у поля пароля, на вкладке «Парольная фраза» поставьте «Количество слов» равным 6 и нажмите «Использовать пароль». *(вывод автора)*
    4. Заблокируйте базу, откройте её и наберите фразу по памяти. Если боитесь забыть, перепишите фразу на бумагу и уберите листок в закрытый ящик дома: это страховка на первое время, а не обязательное условие.

    Пароль, который приходится набирать руками, например на телевизоре, — другой случай: для него берите три случайных слова, как советует NCSC.[5] Мастер-пароль менеджера сюда не относится: это длинная придуманная фраза из темы «Пароли». Подробнее.

6. **Включите вторую защиту на почте.** Это одноразовый код при входе: даже узнав пароль, вор не войдёт без кода, если вы никому его не назовёте. Почта важнее всего: через неё сбрасывают пароли от остальных сайтов. Коды берите из прило-

[3] CISA: Use strong passwords, на англ. Проверено: 2026-10-13.

[4] KeePassXC: страница загрузки, кнопки «Download for Windows» и «Download for macOS», на англ. Проверено: 2026-10-13.

[5] NCSC: Three random words, три случайных слова для пароля; менеджер паролей там назван как другой вариант, на англ. Проверено: 2026-10-13.

жения 2FAS (выбор объяснён в теме «Двухфакторная аутентификация»).

1. Поставьте 2FAS: Google Play на Android, App Store на iPhone.
2. Для Gmail откройте myaccount.google.com, выберите «Безопасность и вход в аккаунт» (или «Безопасность»), в блоке «Вход в Google» нажмите «Включить двухэтапную аутентификацию» и пройдите шаги Google, указав свой номер телефона.[6]
3. На странице «Двухэтапная аутентификация» нажмите «Настроить Authenticator» (на некоторых устройствах сначала «Начать»).[7]
4. Когда Google покажет QR-код, откройте 2FAS, нажмите «+» (на Android внизу справа, на iPhone вверху справа), затем «Scan a QR Code» и наведите камеру на экран.[8] Введите на странице Google код из 2FAS. Результат: при входе с нового устройства почта спрашивает не только пароль.
5. Там же найдите «Резервные коды», нажмите стрелку справа и выберите «Получить резервные коды»; запишите их на бумагу и уберите листок в закрытый ящик дома. Коды одноразовые: они впустят в почту, если телефон потерян.[9]

Если у сервиса нет кодов из приложения, выберите код по СМС. *(вывод автора)* Другая почта и банк: у банка и у других почтовых сервисов пункты свои, их разбор в теме «Двухфакторная аутентификация»; там же копия 2FAS на случай поте-

[6]Справка Google: включение двухэтапной аутентификации, блок «Вход в Google», кнопка «Включить двухэтапную аутентификацию»; название раздела в справках Google различается («Безопасность и вход в аккаунт» и «Безопасность и вход»), поэтому на экране ищите раздел «Безопасность». Проверено: 2026-10-13.

[7]Справка Google: приложение Authenticator для двухэтапной аутентификации, «Настроить Authenticator», на некоторых устройствах «Начать». Проверено: 2026-10-13.

[8]2FAS Auth: учебник, значок «+» (на Android внизу справа, на iOS вверху справа) и пункт «Scan a QR Code», на англ. Проверено: 2026-10-13.

[9]Справка Google: резервные коды, набор из 10 кодов, 8 цифр, каждый одноразовый. Проверено: 2026-10-13.

ри телефона. Подробнее.

7. **Разрешите телефону обновляться самому.** В обновлениях закрывают уязвимости. Часть из них злоумышленники уже используют: CISA ведёт каталог таких уязвимостей.[10] Настройка занимает около 3 минут. *(вывод автора)*

   - iPhone. Откройте `Settings` / `Настройки` ⊠ «Основные» ⊠ «Обновление ПО» ⊠ «Автообновление» и включите «Устанавливать автоматически».[11] Затем «Настройки» ⊠ «Приложения» ⊠ `App Store` ⊠ включите «Обновления приложений» (на английском App Updates).[12]
   - Android. Откройте Google Play, нажмите фото профиля вверху справа ⊠ «Настройки» ⊠ «Настройки подключения» ⊠ «Автообновление приложений» и выберите «Обновление только через Wi-Fi».[13] Систему проверьте так: «Настройки» ⊠ «Система» ⊠ «Обновления ПО» (на Pixel пункт может называться «Обновление системы»); большинство обновлений ставятся сами.[14]

   Если телефон просит перезагрузиться, перезагрузите его вечером; обновление применится после перезапуска. Пункты меню у разных производителей Android различаются: найдите «обновление» через поиск в настройках. Подробнее.

8. **Сохраните фотографии не только на телефоне.** Телефон теряется, ломается и тонет, а снимки детей и родителей не вернуть. Включите копирование в облако своей платформы.

[10] CISA: Known Exploited Vulnerabilities Catalog, на англ. Проверено: 2026-10-13.

[11] Справка Apple: автоматическое обновление iOS, «Настройки» ⊠ «Основные» ⊠ «Обновление ПО» ⊠ «Автообновление», переключатель «Устанавливать автоматически». Проверено: 2026-10-13.

[12] Справка Apple: автоматические обновления приложений на iPhone, путь Settings > Apps > App Store и переключатель App Updates, на англ.; русские подписи страница не приводит. Проверено: 2026-10-13.

[13] Справка Google Play: автообновление приложений, фото профиля ⊠ «Настройки» ⊠ «Настройки подключения» ⊠ «Автообновление приложений», варианты обновления. Проверено: 2026-10-13.

[14] Справка Android: обновление системы, путь Settings > System > Software updates; большинство обновлений на Pixel ставятся автоматически, на англ.; русские подписи страница не приводит. Проверено: 2026-10-13.

- iPhone. «Настройки» ⊠ ваше имя ⊠ iCloud ⊠ «Фото» и включите «Синхронизация этого iPhone».[15]
- Android. Откройте приложение «Google Фото», нажмите значок профиля вверху, откройте настройки Google Фото и включите «Копирование в облако».[16]

Проверка: выйдите из настроек и зайдите снова — переключатель остался включённым. Если облако пишет, что места не хватает, копирование остановилось: смотрите тему «Резервные копии». Подробнее.

9. **Ставьте программы только из проверенных источников.** Файл «бесплатно, без регистрации» с неизвестного сайта может принести в придачу вирус.

    1. На телефоне: App Store (iPhone) или Google Play (Android). Другие источники не используйте.
    2. На компьютере: сначала встроенный магазин (Microsoft Store, магазин на Mac).
    3. Нет в магазине — официальный сайт разработчика. Адрес берите из карточки программы в Википедии, а не из поиска. *(вывод автора)*

    Нет ни в магазине, ни на официальном сайте — не ставьте. Подробнее.

10. **Сомневаетесь — остановитесь и спросите.** Спешка и фраза «только сейчас» — частый приём мошенников: им нужно, чтобы вы не успели подумать. *(вывод автора)* Подождите час и покажите сообщение близкому человеку. Это не стыдно, так делают многие.

> **Максимум**

[15] Справка Apple: настройка Фото iCloud на всех устройствах, «Настройки» ⊠ имя ⊠ iCloud ⊠ «Фото», переключатель «Синхронизация этого [устройства]». Проверено: 2026-10-13.

[16] Справка Google Фото: как проверить резервное копирование, значок профиля вверху, настройки Google Фото, пункт «Копирование в облако» должен быть включён; страница не различает Android и iPhone. Проверено: 2026-10-13.

Дополнительно (на выбор). Берите только то, что подходит вам; красный список выполнен и без этого.

- *Вопросы-ловушки вместо контрольного слова* — если близкие не хотят слово. Заранее договоритесь о двух-трёх невинных вопросах про то, чего нет: «как там Вулфи?» (собаки давно нет), «не забыл полить цветы у бабушки?». Спросите вскользь: свой человек удивится, подделка может поддакнуть. *(вывод автора)* Вопросы не пишите в соцсетях. Подробности — в теме «Безопасность при использовании ИИ».
- *Аппаратный ключ вместо кодов из приложения* — если хотите защитить почту сильнее. Как выбрать и настроить ключ, разобрано в теме «Двухфакторная аутентификация».
- *Перенос фотографий на компьютер вместо облака* — если не хотите хранить снимки у облачного сервиса или не хотите платить за место. Копируйте их на компьютер и держите ещё одну копию на внешнем диске, как в теме «Резервные копии».

Когда красный список выполнен, переходите к темам гайда: в каждой есть конкретное действие, которое можно выполнить сразу. Начните с темы «Пароли».

Прежде чем начать

Порядок один, и он не меняется:

1. Прочитайте «Красный список» — 10 минут.
2. Откройте тему «Пароли» — 15 минут. Украденные и повторно используемые пароли — один из самых частых путей в чужие аккаунты (по отчёту Verizon DBIR 2025, взломанные учётные данные — начальный вектор в 22% утечек),[17] и эта тема закрывает их в первую очередь.
3. Дальше идите по темам в том порядке, в котором они стоят в оглавлении.

В гайде девять основных тем и бонусная десятая тема «Основы работы с нейросетями»; в каждой есть конкретное действие, которое можно выполнить сразу. Время каждой темы указано в её шапке: основные темы занимают от 10 до 24 минут, вместе 142 минуты. Темы идут в порядке, который мы считаем разумным: сначала то, что даёт больше защиты за меньшее время. Остановиться можно после любой темы.

[17] Verizon: Credential stuffing attacks, 2025 DBIR, на англ. Данные отчёта относятся к организациям, не к домохозяйствам. Проверено: 2026-10-11.

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 пароль из переписки и сменить его — 3 минуты
- ☐ Перенести в базу первый из пяти важных сайтов (банк) — 5 минут

Зачем не один пароль

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 популярных 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.

Поставить менеджер паролей

Решение звучит подозрительно просто: запоминать надо один пароль, а не тридцать. Остальные хранит программа — менеджер паролей, база, запертая на этот единственный пароль. Берите KeePassXC: он открытый и бесплатный,[18] а главное — база лежит обычным зашифрованным файлом `.kdbx`,[19] который вы будете хранить в папке «Документы», а копию в облаке сделаете в разделе про телефон. Другие менеджеры — в блоке «Максимум» в конце раздела про телефон.

Установка

1. Откройте страницу keepassxc.org/download.
2. Нажмите `Download for Windows` (Windows) или `Download for macOS` (macOS).[20] На Linux найдите блок `Flatpak Package - Recommended`: в нём указана команда установки.
3. Windows: запустите скачанный файл `.msi` и следуйте шагам установщика. macOS: откройте скачанный файл `.dmg` и установите программу по подсказке в открывшемся окне. Linux: выполните в терминале `flatpak install --user flathub org.keepassxc.KeePassXC`.
4. Откройте KeePassXC. Результат: программа запускается, но базы пока нет.

Если сайт предлагает другой файл или просит оплату, вы не на keepassxc.org: вернитесь по ссылке из шага 1. *(вывод автора)*

[18] KeePassXC User Guide, лицензия GPLv3, на англ. Проверено: 2026-10-11.

[19] KeePassXC Getting Started Guide, зашифрованный файл kdbx, на англ. Проверено: 2026-10-11.

[20] KeePassXC: страница загрузки, кнопки «Download for Windows» и «Download for macOS», блок «Flatpak Package - Recommended» для Linux, на англ. Проверено: 2026-10-13.

Создание базы

1. Нажмите Create new database / Создать новую базу данных.
2. В имени базы введите Пароли, описание не заполняйте. Нажмите Continue / Продолжить. (☒ создание базы).
3. На экране Encryption Settings / Параметры шифрования оставьте формат KDBX 4 и поставьте Decryption Time / Время расшифровки на 3 секунды; вкладку Advanced не открывайте.[21] Нажмите Continue / Продолжить.
4. Дальше откроется экран с мастер-паролем: его шаги — в следующем разделе. Файл базы вы сохраните там же, после кнопки Done.

KeePassXC — настольная программа для Windows, macOS и Linux.[22] Официального мобильного приложения KeePassXC нет: на Android и iOS используют совместимые сторонние клиенты, поэтому их интерфейс может отличаться.

Видео: Теплица социальных технологий — KeePassXC: обзор менеджера паролей с автономным размещением базы паролей https://www.youtube.com/watch?v=CRM93f377Q4

Теплица социальных технологий — KeePassXC: обзор менеджера паролей с автономным размещением базы паролей — подсказка к этому сценарию; названия элементов интерфейса могут отличаться от текущей версии.

- 1:05 — создание базы
- 1:57 — первая запись
- 2:26 — генератор
- 2:44 — копирование пароля в форму сайта
- 4:56 — файл базы в синхронизируемой папке облака

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

[21] KeePassXC User Guide, раздел Creating Your First Database: на экране Encryption Settings гайд не рекомендует менять ничего, кроме ползунка Decryption Time, на англ. Проверено: 2026-10-13.

[22] KeePassXC: страница загрузки, версии для Windows, macOS и Linux, на англ. Проверено: 2026-10-11.

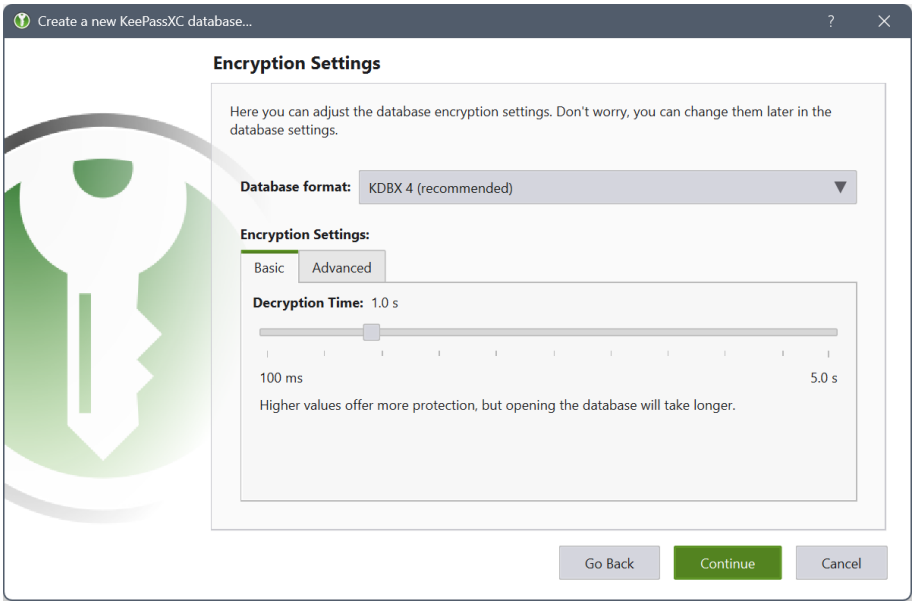


Рис. 1: Экран Encryption Settings / Параметры шифрования KeePassXC: Decryption Time / Время расшифровки

Создать базу и мастер-пароль

Мастер-пароль — единственное, что нужно помнить самому: остальное хранит программа. Поэтому берите такой, который вы сможете запомнить: придуманную вами фразу, а не набор слов с бумажки. Страх забыть главный пароль понятен: в базе будет почта и всё остальное. Но пароль вы набираете при каждом открытии базы, и обычно он запоминается за неделю-две. *(вывод автора)* Пока вы в нём не уверены, есть страховка — листок в закрытом месте (шаг 5); это помощь на первое время, а не обязательное условие.

Придуманная фраза должна быть длинной и новой. Файл базы можно скопировать и подбирать пароль к нему дома, на мощных компьютерах, хоть годами: время расшифровки только замедляет каждую попытку. Выдержит база или нет, решает одно — насколько фраза непредсказуема. Человек выбирает хуже генератора: любимые слова, даты, цитаты и соседние клавиши перебирают первыми. *(вывод автора)* Поэтому у придуманной фразы жёсткие условия, они в первом шаге: длина, слова, которые раньше не встречались вместе, и проверка оценкой KeePassXC. Если не хотите придумывать сами, ниже есть вариант, где фразу выдаёт программа.

Иллюстрация: Database Credentials / Доступ к базе данных; значок кубика (A) в поле пароля запускает генератор.

1. Придумайте фразу, пока не вводя её в программу:
   - из нескольких слов, которые раньше не встречались вместе; вместе с цифрами и символами из последнего пункта она должна быть длиннее 20 символов;
   - не из книги, песни, известного текста или популярной цитаты; без имени, даты рождения и других личных данных; не из соцсетей; не пароль с другого сайта;
   - наберите её при включённой английской раскладке (пример ниже) и добавьте цифры и 1–2 спецсимвола, например `!"#;%:?*()`.
2. В окне `Database Credentials` / `Доступ к базе данных` наберите фразу в поле `Enter password` / `Введите пароль`.
3. Повторите фразу в поле `Confirm password` / `Подтвердите`

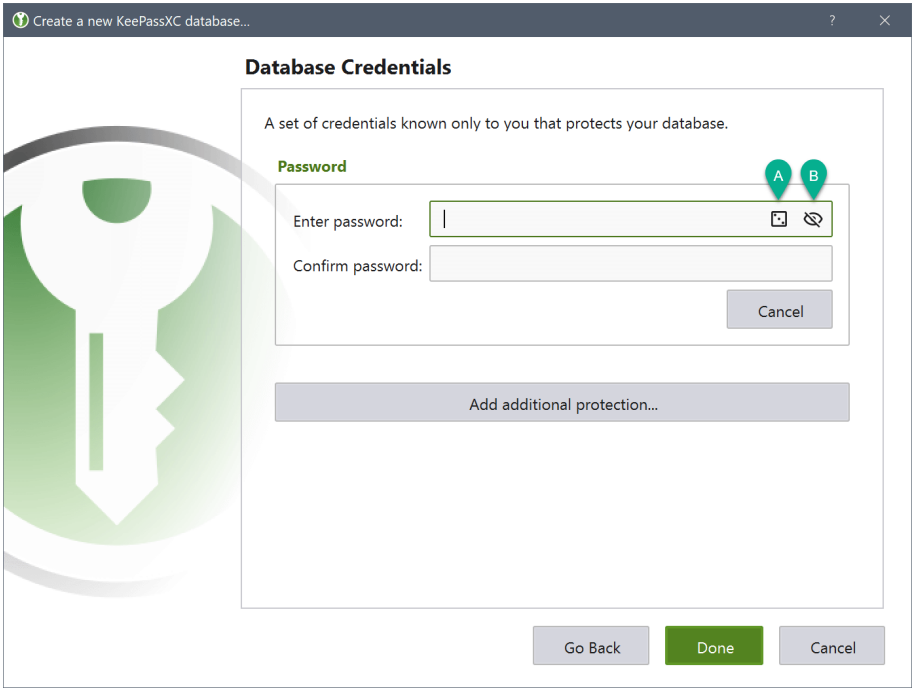


Рис. 2: Окно Database Credentials / Доступ к базе данных KeePassXC

пароль.

4. Проверьте оценку KeePassXC: не ниже 75 bit (ниже KeePassXC считает пароль слабым, Weak).[23] В окне мастера числа нет, оно показывается в генераторе паролей: как его там получить, написано сразу после шагов. Если оценка ниже, добавьте к фразе слова, пока она не дойдёт до 75.
5. Если боитесь забыть, перепишите фразу на бумагу и положите листок в закрытый ящик или сейф дома. Не фотографируйте его, не храните в телефоне, облаке и рядом с файлом .kdbx. Когда начнёте набирать фразу уверенно, листок можно уничтожить либо оставить как аварийный офлайн-резерв в закрытом месте. *(вывод автора)*
6. Нажмите кнопку Done — последнюю в мастере. В окне сохранения выберите папку «Документы», введите имя Пароли.kdbx и нажмите Save / Сохранить.[24]
7. Проверьте: нажмите Database / База данных -> Lock Database / Заблокировать базу, затем откройте файл Пароли.kdbx и введите фразу по памяти. Повторите завтра и через несколько дней, не подглядывая: так фраза закрепляется. *(вывод автора)*

Результат: база открывается только с мастер-паролем, и вы можете набрать его по памяти. Если фраза не подходит, вы набираете её не так, как придумали: проверьте раскладку, регистр и спецсимволы; если есть листок, сверьтесь с ним символ за символом. *(вывод автора)*

Как измерить энтропию выбранного мастер-пароля прямо в KeePassXC. В окне Database Credentials / Доступ к базе данных числа нет: под полем Enter password / Введите пароль видна только тонкая цветная полоска, а слово качества («Качество: Хороший») появляется подсказкой при наведении мыши.[25] Число

[23] KeePassXC, исходный код оценки пароля (PasswordHealth.cpp): ниже 40 бит качество Poor, от 40 до 75 бит Weak, от 75 до 100 бит Good, от 100 бит Excellent, на англ. Проверено: 2026-10-13.

[24] KeePassXC User Guide, раздел Creating Your First Database: кнопка Done, затем окно сохранения файла .kdbx, на англ. Проверено: 2026-10-13.

[25] KeePassXC 2.7.12, исходный код, на англ.: PasswordWidget.cpp (полоска качества под полем пароля, подсказка «Quality: …», числа в подписи нет); PasswordWidget.ui (высота полоски 4 пикселя); PasswordEditWidget.cpp (полоска

в битах показывает окно генератора паролей: поле в нём можно редактировать, и программа оценивает то, что в нём набрано. Так можно измерить свою фразу прямо во время создания базы:

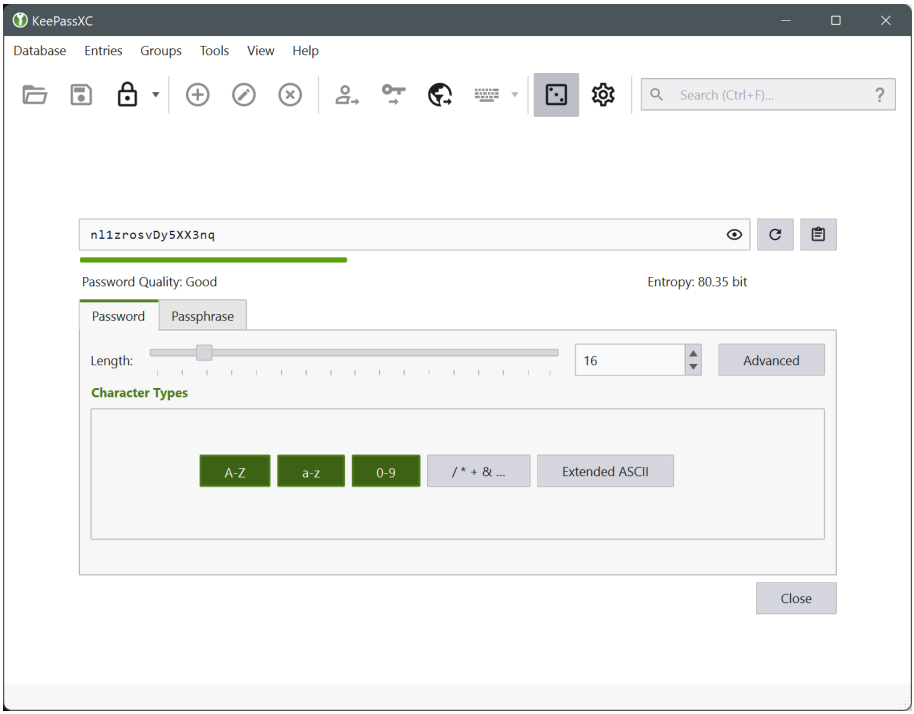


Рис. 3: Окно генератора паролей KeePassXC: под полем пароля подписи Password Quality / Качество пароля и Entropy / Энтропия

Иллюстрация: генератор паролей, вкладка Password / Пароль. Под полем две подписи: Password Quality / Качество пароля и Entropy / Энтропия, в битах. В поле на скриншоте случайный пароль, выданный программой; поле то же самое, в нём можно набрать свою фразу.

1. Когда вы дошли до шага 4, нажмите значок кубика в правой части поля `Enter password` / `Введите пароль`: откроется окно генератора. Вне мастера оно открывается из главного

включена у поля пароля мастера); PasswordGeneratorWidget.ui (у поля пароля генератора нет признака «только чтение»); PasswordGeneratorWidget.cpp (подпись `Entropy: %1 bit`). Проверено: 2026-10-22.

окна: Tools / Сервис -> Password Generator / Генератор паролей. Пока окно генератора открыто из мастера, меню главного окна недоступно.[26]

2. Откройте вкладку Password / Пароль, не Passphrase / Парольная фраза: на второй число считается по настройкам генератора, а не по тексту в поле.[27]
3. Щёлкните в поле, выделите выданный случайный пароль (Ctrl + A, на macOS ⌘ + A) и наберите свою фразу так, как набираете её в мастере: английская раскладка, цифры и спецсимволы. Если вместо символов точки, нажмите значок глаза справа в поле. После ввода не трогайте ползунок, флажки и кнопку обновления: любая смена настроек заменяет текст в поле новым случайным паролем.[28]
4. Прочитайте подписи под полем: Password Quality / Качество пароля и Entropy / Энтропия (в англоязычном интерфейсе Entropy: … bit). Вам нужно не ниже 75 bit: это качество «Хороший» (Good); от 40 до 75 бит «Слабый» (Weak), ниже 40 «Плохой» (Poor), от 100 «Отличный» (Excellent).
5. Если число ниже, добавьте к фразе слова прямо в этом поле и смотрите, как оно растёт. Затем внесите те же слова в поле мастера.
6. Закройте окно кнопкой Close / Закрыть, кнопку копирования не нажимайте. Кнопка Apply Password / Использовать пароль подставит содержимое поля генератора в оба поля мастера: нажимайте её, только если в поле ваша фраза, а не

[26] KeePassXC 2.7.12, на англ.: PasswordWidget.cpp (значок кубика открывает генератор); PasswordGeneratorWidget.cpp (окно из мастера открывается с Qt::ApplicationModal, то есть блокирует остальные окна программы); PasswordGenerator.adoc (Tools > Password Generator); русские подписи: keepassxc_ru.ts («Сервис», «Генератор паролей», «Закрыть»). Проверено: 2026-10-22.

[27] KeePassXC 2.7.12, PasswordGeneratorWidget.cpp, updatePasswordStrength(): на вкладке Passphrase энтропия берётся из estimateEntropy() генератора, на вкладке Password из PasswordHealth(текст поля), на англ. Проверено: 2026-10-22.

[28] KeePassXC 2.7.12, PasswordGeneratorWidget.cpp: смена вкладки, слайдера, флажков и списка слов вызывает updateGenerator(), а он regeneratePassword(), который записывает в поле новый пароль; значок глаза: PasswordWidget::setShowPassword() в PasswordWidget.cpp, на англ. Проверено: 2026-10-22.

случайный пароль.[29]

Что значит число. Бит здесь — степень двойки: `75 bit` это оценка в 2^75 (около $4 \cdot 10^{22}$) вариантов, которые придётся перебрать подбирающему, а каждый лишний бит удваивает работу. Ориентиры: 75 бит — минимум этой главы; фраза из 6 слов генератора даёт 77.54 бит (считается по формуле для случайных слов, а не по тексту); фраза, которую вы набрали сами, получает оценку другим способом (по тексту), поэтому даже те же шесть слов, набранные вручную, покажут другое число.

Число не заменяет условий шага 1. Оценка считается только по тексту в поле: KeePassXC не передаёт в неё ни ваше имя, ни дату рождения, ни список известных цитат.[30] Такая оценка вам не скажет, что фраза взята из песни, книги или соцсетей, или что в ней ваши личные данные; такую фразу перебирают раньше случайной, хотя число в подписи может быть высоким. *(вывод автора)* Поэтому сначала выполняются условия шага 1 (новая фраза, не цитата, ничего личного), а `75 bit` проверяет только то, что они не свелись к слишком короткому тексту.

Мастер-пароль нельзя класть в ту же базу: он нужен, чтобы её открыть. Копии файла базы (раздел «Сохранить базу») защищают от потери файла, но не от забытой фразы: от этого страхует только листок из шага 5.

На телефоне такой мастер-пароль набирается на английской раскладке. Это единственная сложность, и её достаточно один раз выучить. Остальные пароли вручную вводить не придётся: базу вы открываете мастер-паролем, а дальше приложение подставляет логины и пароли само. Как открыть базу на телефоне — в разделе про несколько устройств.

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

[29] KeePassXC 2.7.12, PasswordWidget.cpp, `popupPasswordGenerator()`: сигнал `appliedPassword` подключён к `setText` и поля пароля, и поля повтора, на англ. Проверено: 2026-10-22.

[30] KeePassXC 2.7.12, PasswordHealth.cpp: энтропия считается вызовом `Zxcvbn Match(текст пароля, nullptr, nullptr)`, пользовательский словарь не передаётся, на англ. Проверено: 2026-10-22.

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

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

Так устроена механика. Саму замену по раскладке защитой считать нельзя: программы подбора умеют прогонять словари через правила, в том числе правила замены символов,[31] и слово, записанное в другой раскладке, для такого перебора лишь один из вариантов. *(вывод автора)* Защищают пароль длина и случайность: фраза из слов, которые раньше не встречались вместе, — а не сама замена. Замена по раскладке нужна для другого: пароль легко запомнить и он однозначный. Вы помните понятную фразу и всегда знаете, какие клавиши нажимать. Поэтому фраза должна быть вашей и новой: известную или предсказуемую фразу замена букв не спасёт.

Это публичный учебный пример. Не копируйте его и не используйте как свой мастер-пароль.

Видео: Первый отдел — Надёжный пароль. Объясняем за 13 минут 37 секунд https://www.youtube.com/watch?v=pAUzloZkxWE

Первый отдел — Надёжный пароль. Объясняем за 13 минут 37 секунд — общий ролик о выборе надёжного пароля; без привязки к конкретному моменту.

Если не хотите придумывать сами: фразу выдаст программа.

[31] Hashcat Wiki: Rule-based Attack, правила изменяют слова словаря, в том числе заменяют символы (функция `s`), на англ. Проверено: 2026-10-25.

Такую фразу запомнить труднее, чем свою, поэтому листок из шага 5 здесь нужен, пока вы не заучите её. *(вывод автора)* Вместо шагов 1–4 сделайте так:

1. Нажмите значок кубика в правой части поля `Enter password` / `Введите пароль`: он запускает встроенный генератор паролей.[32] (⚄ генератор).
2. Откройте вкладку `Passphrase` / `Парольная фраза` и поставьте `Word Count` / `Количество слов` равным 6. Подпись под полем покажет «Энтропия … бит»: для 6 слов это 77.54 бит (log2 от 7772 слов словаря, умноженный на 6). Шесть слов — минимум, который советует EFF для фразы из словаря такого размера;[33] меньше не ставьте. Значение по умолчанию (7 слов, 90.47 бит) тоже подходит.[34][35]
3. Нажмите `Apply Password` / `Использовать пароль` и повторите фразу в поле `Confirm password` / `Подтвердите пароль`. Дальше — шаги 5–7 выше.

Берите фразу ровно такой, какой её выдал генератор: он берёт числа у криптографического генератора случайных чисел,[36] и ваш «вклад» случайность не добавляет, а портит. Не правьте слова, не меняйте их местами и не нажимайте кубик снова и снова, пока не выпадет «красивая»: выбирая из выпавшего, вы выбираете сами. *(вывод автора)*

Проверь себя. Что нужно сделать при создании базы?

---

[32] KeePassXC User Guide, значок кубика в поле пароля запускает генератор паролей, на англ. Проверено: 2026-10-13.

[33] EFF: Dice-Generated Passphrases, «We recommend selecting a minimum of six words from our long wordlist», на англ. Проверено: 2026-10-13.

[34] KeePassXC, исходный код генератора парольных фраз (PassphraseGenerator.cpp): энтропия равна log2(число слов в словаре), умноженному на число слов; по умолчанию 7 слов и словарь eff_large, на англ. Проверено: 2026-10-13.

[35] KeePassXC, словарь eff_large.wordlist, в файле 7772 слова (log2(7772) = 12,924 бит на слово), на англ. Проверено: 2026-10-13.

[36] EFF: Dice-Generated Passphrases: пять бросков кубика на слово из длинного списка; KeePassXC, исходный код генератора (PassphraseGenerator.cpp), слова выбираются через `randomGen()`; Random.cpp: байты берёт генератор Botan (системный `System_RNG`, если он доступен при сборке, иначе `Autoseeded_RNG`); `openssl rand` — man openssl-rand, на англ. Проверено: 2026-10-16.

1. Придумать пароль из одного слова и добавить в конец цифру.
2. Придумать новую фразу из слов, которые раньше не встречались вместе, проверить оценку не ниже `75 bit`, подтвердить её в окне `Database Credentials` / `Доступ к базе данных` и проверить, что набираете её по памяти.
3. Положить мастер-пароль в новую запись той же базы.

Второй. Длинная фраза из слов, не встречавшихся вместе, с оценкой не ниже 75 бит устойчива к подбору, а запоминается за неделю-две ежедневного набора. Листок, если он нужен, храните в закрытом месте отдельно от файла базы, а мастер-пароль в саму базу не кладите.

Получилось — когда файл базы создан, а мастер-пароль от него вы набираете по памяти (или с листка, пока не запомнили).

> **Максимум**
>
> **Дополнительно: случайность без программы — кубик и `openssl`.** Генератор KeePassXC работает через библиотеку Botan и обычно опирается на генератор самой операционной системы. Если не доверяете программе или хотите выбрать слова без компьютера, бросайте кубик: на каждое слово пять бросков по списку EFF (6 слов — 30 бросков, это те же 77,5 бит); слова берите ровно те, что выпали. Случайный набор байт для ключа (скажем, файла-ключа вне KeePassXC) даёт команда `openssl rand -hex 32` на macOS и Linux: это 32 байта, 256 бит, из криптографического генератора OpenSSL, который заполняется из источника случайности операционной системы. Файл-ключ в KeePassXC создавайте кнопкой «Генерировать» (см. блок ниже), а не из своей картинки или текста.

> **Максимум**
>
> **Дополнительно: время расшифровки.** Время расшифровки увеличивает стоимость каждой проверки мастер-пароля и каждой офлайн-попытки взлома украденного файла. Слиш-

ком 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 обязательное требование KeePassXC. Время растёт примерно пропорционально числу итераций; на другом устройстве оно будет другим, 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 оставьте не ниже 1 секунды. *(вывод автора)*

- ☐ В мастере создания базы поставить время расшифровки на 3 секунды; вкладку `Advanced` не менять.

Максимум

Дополнительно: файл-ключ. 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 ключевой файл` -> `Generate` / `Генерировать`, сохраните файл отдельно от `.kdbx`, сделайте отдельную копию и проверьте открытие с мастер-паролем и key file. Для восстановления копия `.kdbx` и соответствующий key file должны быть доступны вместе, но храниться в разных 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

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

[a] KeePassXC User Guide, раздел о ключах базы: аппаратные ключи YubiKey и OnlyKey, добавление «Add YubiKey Challenge-Response», на англ. Проверено: 2026-10-12.

Придумать пароль для сайта

Иллюстрация: Password Generator / Генератор паролей для обычного пароля записи; тот же встроенный генератор может выдать и парольную фразу для мастер-пароля, если не хочется придумывать её самому.

Для каждой обычной записи не придумывайте пароль вручную:

1. Нажмите `New Entry...` / `Создать запись...` (меню `Entries` / `Записи`). (⊠ первая запись).
2. Заполните поля `Title` / `Название`, `Username` / `Логин` и `Password` / `Пароль`.
3. Нажмите значок кубика в поле пароля. (⊠ генератор).
4. Сгенерируйте пароль и проверьте оценку: не ниже `128 bit`. Если ниже, увеличьте значение `Length` / `Длина`, пока оценка не дойдёт до 128.
5. Нажмите `Apply Password` / `Использовать пароль`, чтобы применить сгенерированный пароль в запись.
6. Заполните `Notes` / `Заметки` (что вписать — в разделе «Записать новый сайт» ниже), нажмите `OK` / `OK`, чтобы закрыть редактор записи, затем `Save` / `Сохранить`, чтобы сохранить ба-

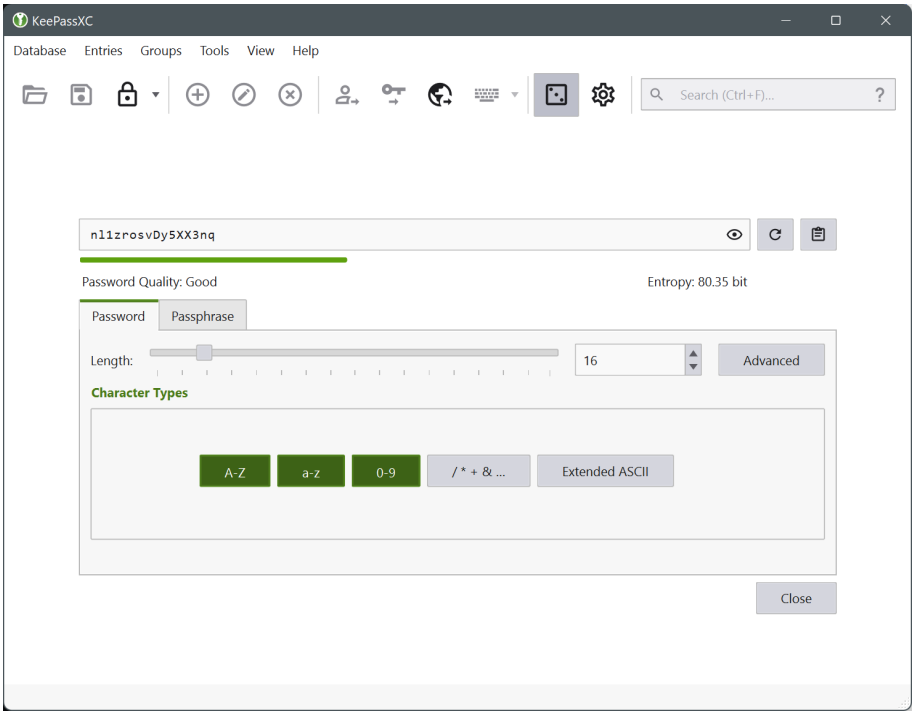


Рис. 4: Окно Password Generator / Генератор паролей KeePassXC для создания пароля записи

зу. Нажимайте Save / Сохранить всегда.
7. Скопируйте пароль через Copy Password / Скопировать пароль, вставьте его в форму официального сайта. KeePassXC сам очистит буфер обмена через заданное время (по умолчанию 10 секунд).[37] (☒ копирование пароля).
8. Результат: в базе сохранена запись с логином и тем же сгенерированным паролем, который был передан сайту.

Максимум

Дополнительно: исключить похожие символы в генераторе. Берите, если пароль придётся читать с экрана и набирать руками: так вы не перепутаете 0 и O или 1, l и I. В пароле на иллюстрации в начале этого раздела есть и l, и 1: в простом режиме генератор их не убирает.

1. Откройте генератор: значок кубика в поле Password / Пароль записи либо Tools / Сервис -> Password Generator / Генератор паролей.
2. Откройте вкладку Password / Пароль: на вкладке Passphrase / Парольная фраза такой настройки нет.
3. Нажмите кнопку Advanced / Дополнительно справа от поля длины: она раскрывает дополнительные настройки. Без этого шага флажок из следующего пункта не действует: флаги исключения программа применяет только в расширенном режиме.[a]
4. Найдите флажок Exclude look-alike characters / Не использовать похожие символы и убедитесь, что он включён (по умолчанию он включён). Если навести на него курсор, программа покажет список исключённых символов: 0, 1, l, I, O, |, B, 8, G, 6.
5. Нажмите кнопку обновления рядом с полем пароля и проверьте оценку под ним: не ниже 128 bit, как в шаге 4 выше. Если ниже, увеличьте значение Length /

[37] KeePassXC, исходный код настроек (Config.cpp): очистка буфера обмена включена по умолчанию, срок ClearClipboardTimeout равен 10 секундам, на англ. Проверено: 2026-10-13.

Длина. Затем нажмите Apply Password / Использовать пароль.

[a] KeePassXC 2.7.12, на англ.: PasswordGeneratorWidget.ui (кнопка «Advanced» на вкладке Password, флажок «Exclude look-alike characters» и подсказка со списком исключённых символов), PasswordGeneratorWidget.cpp (generatorFlags(): флаг ExcludeLookAlike выставляется только при включённом расширенном режиме), Config.cpp (значение по умолчанию: включено), keepassxc_ru.ts («Не использовать похожие символы», «Дополнительно»). Проверено: 2026-10-25.

Максимум

Дополнительно: пароль придётся вводить руками (телефон, телевизор, приставка). Обычный пароль копируют и вставляют, поэтому его вид не важен. Но бывают места, где копировать нечем и пароль набирают пальцем или пультом. Для них:

- Берите режим Passphrase / Парольная фраза: пароль из слов набирать и проверять глазами проще, чем такую же по силе кашу из символов. Берите не меньше 6 слов. *(вывод автора)*
- Если нужен пароль из символов, а не из слов, исключите похожие символы 0 и O или 1, l и I, которые легко перепутать: порядок описан в блоке выше, в русском интерфейсе флажок называется «Не использовать похожие символы».[a]
- Для малоценных аккаунтов, где сервис режет длину или не принимает спецсимволы (на телевизорах такое бывает), берите длину не меньше 12 символов; если сервис не принимает и столько, ставьте максимум, который он принимает. Главное, чтобы пароль нигде больше не повторялся. *(вывод автора)*

[a] KeePassXC, исходный код окна генератора паролей (PasswordGeneratorWidget.ui) (флажок «Exclude look-alike characters») и русский перевод интерфейса (keepassxc_ru.ts) («Не использовать похожие символы»), на англ. Проверено: 2026-10-12.

Подключить расширение браузера

Сама программа в браузерную форму автоматически не подставляет — подставлять логин и пароль прямо в форму на сайте умеет расширение для браузера. Поставьте расширение в свой основной браузер: с ним пароль подставляется сам, 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 — Brave устанавливает расширения из Chrome Web Store.
- KeePassXC Browser — тот же Chrome Web Store — другие браузеры на базе Chromium: откройте страницу расширения в Chrome Web Store и установите его оттуда, подтвердив разрешения.
- Документация KeePassXC — для Safari поддержка расширения пока предварительная: подробности в блоке «Максимум» ниже.

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`: на Windows и Linux — меню `Tools` / `Сервис` -> `Settings` / `Настройки`, на macOS — сочетание ⌘ и запятой.[38]

[38] KeePassXC User Guide, настройки приложения открываются через Tools ⌘ Settings, сочетание Ctrl + , (на macOS Cmd вместо Ctrl), на англ. Проверено: 2026-10-13.

2. Перейдите на вкладку `Browser Integration` / `Интеграция с браузерами`, включите `Enable browser integration` / `Включить интеграцию с браузерами`, отметьте галочкой тот браузер, для которого вы поставили расширение (в списке он показан под своим обычным названием — Google Chrome, Firefox и так далее, без перевода), и нажмите `OK` / `OK`. (☒ интеграция с браузерами).

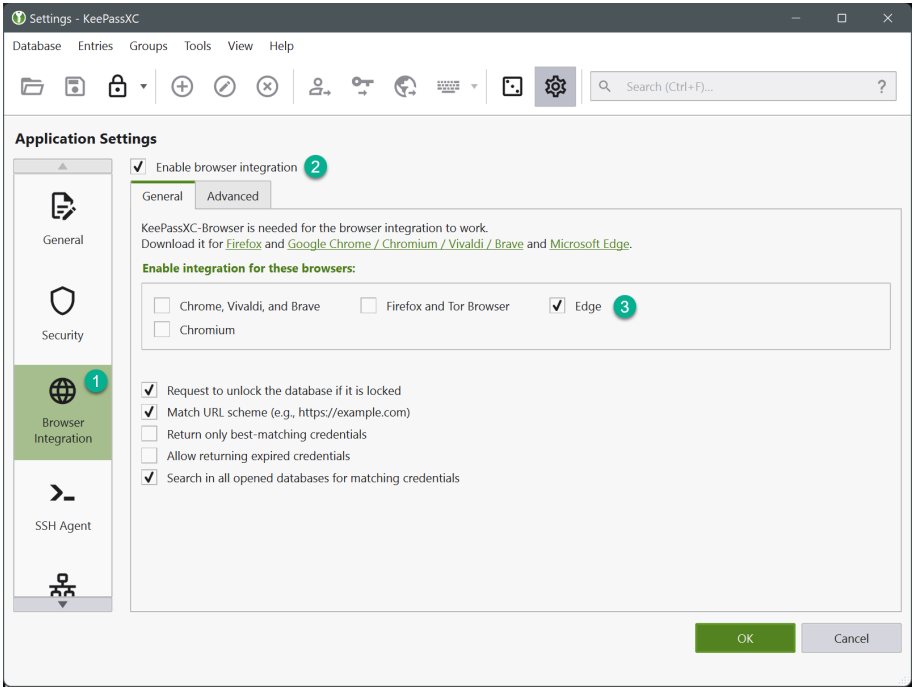


Рис. 5: Окно Application Settings / Настройки приложения KeePassXC: вкладка Browser Integration / Интеграция с браузерами

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 расши-

рений — значок «кусочек пазла») и нажмите Connect.[39] (☒ подключение расширения).

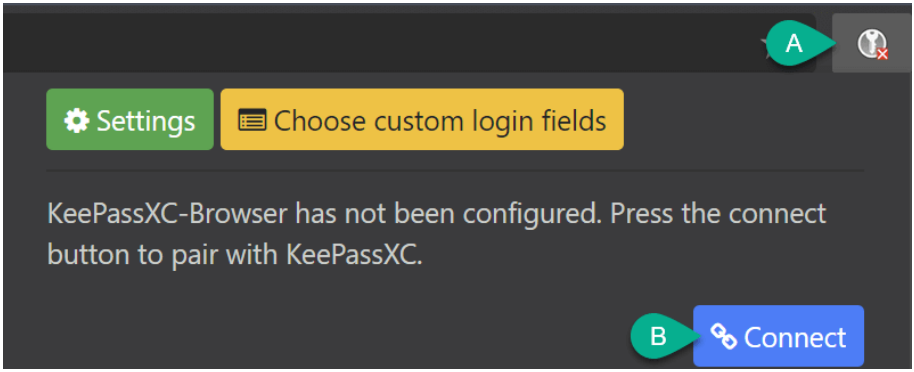


Рис. 6: Всплывающее окно расширения KeePassXC-Browser до подключения к KeePassXC

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 название по образцу «браузер-устройство», например firefox-laptop, 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.

Видео: Инфобездна — Менеджер паролей на все устройства с синхронизацией на базе KeePassXC https://www.youtube.com/watch?v=hc66uupPHGM

Инфобездна — Менеджер паролей на все устройства с синхронизацией на базе KeePassXC — подсказка к подключению расширения

[39] KeePassXC User Guide, раздел Browser Integration: кнопка Connect, имя связки (например, firefox-laptop), кнопка Save and allow access, на англ. Проверено: 2026-10-13.

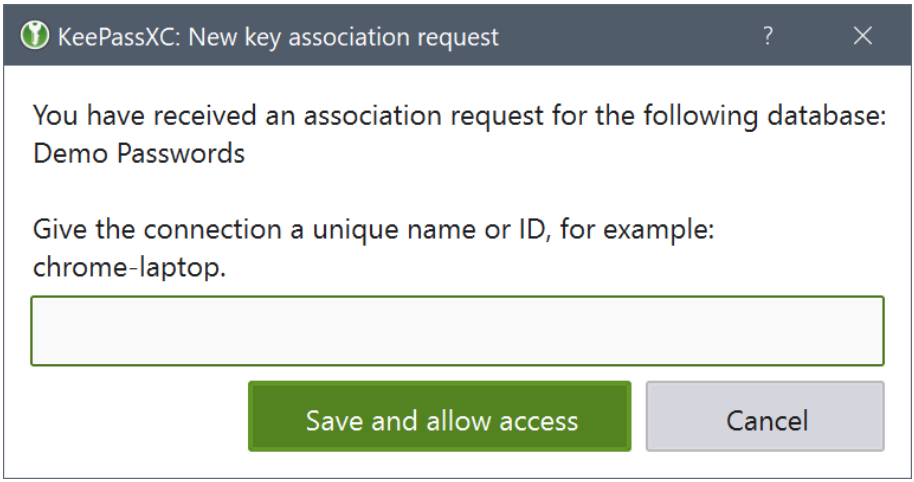


Рис. 7: Диалог New key association request / Запрос на ассоциацию нового ключа KeePassXC

браузера и к открытию базы на телефоне; в ролике база лежит в OneDrive и открывается в другом приложении для телефона, названия элементов могут отличаться.

- 5:00 — интеграция с браузерами в настройках KeePassXC
- 5:17 — подключение расширения
- 7:18 — открыть базу на телефоне

Чтобы автозаполнение сработало, 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 входа.

> **Максимум**
>
> **Дополнительно: второй браузер, второй компьютер.** Повторите установку расширения и шаги 3–4 в каждом браузере, где нужна подстановка: в другом браузере на этом компью-

тере и на втором ноутбуке (на нём предварительно нужна своя копия KeePassXC и базы). Связка работает отдельно для каждого браузера и каждого устройства. На телефоне и планшете расширение не нужно: подстановку там делает приложение для баз KeePass через системное автозаполнение, как включить его — в разделе про несколько устройств.

Максимум

Дополнительно: Safari. Поддержка Safari в расширении «предварительная» (с версии 1.10.0, март 2026).[a] Порядок установки расширения для Safari здесь не описан: откройте страницу релизов по ссылке в сноске и ориентируйтесь на неё. Пока поддержка предварительная, можно обойтись без расширения: встроенный в KeePassXC Auto-Type вводит логин и пароль в активное окно, в том числе в Safari. *(вывод автора)*

[a] keepassxc-browser: релиз 1.10.0 на GitHub, 4 марта 2026, пункт «Add preliminary support for Safari», на англ. Проверено: 2026-10-13.

Записать новый сайт

Запись в базе — это не только пароль. Через год вы не вспомните, на какую почту оформлен кабинет, на чьё имя куплена подписка и когда вы там зарегистрировались. Заведите привычку заполнять одни и те же поля:

- **Название ресурса** — поле `Title` / `Название`, так, как вы сами это называете («Почта основная»).
- **Адрес страницы входа** — поле `URL`: настоящий адрес, скопированный с официального сайта.
- **Логин** — поле `Username` / `Логин`.
- **Пароль** — поле `Password` / `Пароль`, из генератора.
- **Почта регистрации**, **телефон**, **ФИО или на кого оформлено** и **дата регистрации** — в поле `Notes` / `Заметки`, каждый пункт с новой строки.

Новую регистрацию ведите по чеклисту:

1. Откройте базу и нажмите New Entry... / Создать запись....
2. Впишите название ресурса, адрес страницы входа и логин.
3. Сгенерируйте пароль с оценкой не ниже 128 bit и примените его в запись.
4. В заметках укажите почту и телефон, на которые регистрируетесь, на кого оформлено и сегодняшнюю дату.
5. Нажмите OK / OK, затем Save / Сохранить: пароль должен оказаться в базе раньше, чем на сайте.
6. Только теперь заполните форму регистрации на сайте, вставив логин и пароль из записи; KeePassXC сам очистит буфер обмена через заданное время.
7. Если регистрация не удалась, выделите запись, нажмите клавишу Del и подтвердите перемещение в корзину: в базе не должно оставаться записей без сайта.[40]

Порядок такой: **сначала все новые регистрации — по этому чеклисту, а потом перенос старых паролей, начиная с почты.** Тогда список старых паролей перестаёт расти, и переезжать остаётся ровно то, что накопилось до сегодняшнего дня.

Максимум

Дополнительно: отдельные поля вместо заметок. Берите, если хотите, чтобы почта, телефон, ФИО и дата регистрации лежали не одним текстом в заметках, а каждое в своём поле со своим названием. KeePassXC умеет добавлять к записи такие поля: в программе они называются «дополнительные атрибуты».[a]

1. Откройте запись двойным щелчком мыши.
2. В списке слева выберите раздел Advanced / Дополнительные: в нём блок Additional attributes / Дополнительные атрибуты.
3. Нажмите Add / Добавить: в списке появится поле «Но-

[40] KeePassXC User Guide, раздел Deleting an Entry: клавиша Del, запрос о перемещении в корзину, на англ. Проверено: 2026-10-13.

вый атрибут» (`New attribute`), и его имя сразу можно править. Впишите имя, например `Почта регистрации`, и нажмите Enter.
4. Выберите поле в списке и впишите значение в окно справа.
5. Повторите для остальных данных: `Телефон`, `ФИО`, `Дата регистрации`. Имя поля меняет кнопка `Edit Name` / `Изменить имя`, лишнее поле убирает `Remove` / `Удалить`.
6. Нажмите `OK` / `OK`, затем `Save` / `Сохранить`.

Значение, которое не должно быть видно на экране, скройте кнопкой `Protect` / `Защитить`: вместо текста будут точки, пока вы не нажмёте `Reveal` / `Показать`.

[a] KeePassXC 2.7.12, на англ.: EditEntryWidgetAdvanced.ui (блок «Additional attributes», кнопки Add, Remove, Edit Name, Protect, Reveal), EditEntryWidget.cpp (страница «Advanced»; `insertAttribute()` создаёт поле «New attribute» и открывает его имя для правки), keepassxc_ru.ts («Дополнительные», «Дополнительные атрибуты», «Добавить», «Изменить имя», «Удалить», «Защитить», «Показать»). Проверено: 2026-10-25.

Начать перенос с почты

Старые пароли переносите после того, как новые регистрации пошли по чеклисту. 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. Ниже шаги для Gmail; другие почтовые сервисы — в блоке «Максимум» после списка.

1. Откройте myaccount.google.com и войдите. В левой части выберите «Безопасность и вход в аккаунт», в разделе «Вход в Google» — «Пароль» (Google может попросить войти ещё раз). Поле нового пароля пока не заполняйте.[41]
2. В KeePassXC откройте существующую запись почты через `Edit Entry` / `Изменить запись`.
3. Нажмите значок кубика в поле пароля, сгенерируйте новый

[41] Справка Google: изменить пароль: «Безопасность и вход в аккаунт» ☒ «Вход в Google» ☒ «Пароль» ☒ «Сменить пароль». Проверено: 2026-10-13.

пароль и проверьте оценку: не ниже `128 bit`.
4. Нажмите `Apply Password` / `Использовать пароль`, чтобы сгенерированный пароль попал в запись.
5. Нажмите `OK` / `OK`, чтобы закрыть редактор записи, затем `Save` / `Сохранить`: первая кнопка закрывает редактор записи, вторая записывает изменения в файл базы. Сохраняйте до смены на сайте.
6. Скопируйте пароль из записи, введите его в форму Google и нажмите «Сменить пароль».
7. Выйдите из почты и войдите снова с логином и паролем из сохранённой записи.
8. Заблокируйте базу.

Если записи нет, сначала используйте полный сценарий обычной записи: `New Entry...` / `Создать запись...`, `Title` / `Название`, `Username` / `Логин`, `Password` / `Пароль`.

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

> **Максимум**
>
> **Дополнительно: другая почта.** В других почтовых сервисах обычно есть раздел «Безопасность» или «Вход и безопасность»; смена пароля лежит в нём. Если не нашли — введите в поиске по настройкам «пароль». Остальные шаги те же: шаги 2–8 списка выше.

Сохранить базу

Держите три экземпляра базы: рабочий файл `Пароли.kdbx` в папке «Документы», копия №1 в облаке — в том, которым вы уже пользуетесь (то же облако, что и в разделе про телефон, копию делаете там), и копия №2 на флешке. *(вывод автора)* Зашифрованный файл `.kdbx` можно хранить в облаке, но мастер-пароль, key file и экспорт не должны лежать рядом с базой в незашифрованном виде. (☒ синхронизация).

Раз в 3 месяца проверяйте копию с флешки: откройте её мастер-паролем и убедитесь, что последние записи на месте. *(вывод автора)* Копия на другом устройстве должна быть именно отдельной проверенной копией, а не единственным синхронизированным двойником.

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` / `Логин` и `Password` / `Пароль` сохранены; пароль не должен быть в чате или заметках браузера.
3. Заблокируйте базу через `Lock Database` / `Заблокировать базу`, и убедитесь, что копия `.kdbx` лежит отдельно от рабочего файла.
4. Результат: база открывается, запись актуальна, а резервная копия существует и не является единственным файлом.

> **Максимум**
>
> **Дополнительно: выбор носителя и облака.** Если нужно версионирование, выбирайте носитель или провайдера с историей версий и автоматическими резервными копиями; если облака у вас нет, замените его второй флешкой, которую храните в другом месте.

Открыть базу на телефоне

KeePassXC удобен на компьютере, но пароли нужны и на телефоне. Если база открывается только за одним ноутбуком, остальное время приходится вспоминать пароли по памяти — и менеджер бросают. Поэтому сразу сделайте так, чтобы базу можно было открыть везде. `.kdbx` — обычный файл, его без труда открывают на других устройствах.

1. Скопируйте (не переносите) `Пароли.kdbx` из папки «Документы» в папку синхронизации облака, которым вы уже пользуетесь. Облако видит только зашифрованный файл, мастер-пароль туда не попадает.
2. Скопируйте `Пароли.kdbx` из «Документов» ещё и на флешку — это копия №2 из раздела выше. Затем дождитесь окончания синхронизации облака.
3. Поставьте приложение из официального магазина: на Android — KeePassDX (открытый код, GPL-3.0, бесплатный),[42] на iOS — KeePassium (открытый код, GPLv3; бесплатный, платная подписка необязательна).[43] Официального мобильного KeePassXC нет, но `.kdbx` открывают совместимые клиенты; интерфейс у них свой.
4. В приложении добавьте существующую базу, укажите файл `.kdbx` из облака и введите мастер-пароль. (⊠ открыть базу на телефоне).
5. Включите автозаполнение. Android, KeePassDX: `Settings` ⊠ `Form filling` ⊠ `Set default autofill service` (в версии 4.2.0 и новее — `Credential provider service`), затем выберите KeePassDX в системном меню автозаполнения.[44] iOS, KeePassium: `Settings` ⊠ `General` ⊠ `AutoFill & Passwords` ⊠ включите `AutoFill Passwords and Passkeys`, выберите KeePassium и снимите отметку с `Apple Passwords`.[45] Вход по отпечатку пальца не включайте (в блоке «Максимум» ниже сказано, как быть, если всё же хотите): мастер-пароль вводите вручную. *(вывод автора)*
6. Откройте несколько групп и записей и проверьте, что они на месте.

Изменения на двух устройствах одновременно могут конфликтовать, поэтому перед редактированием убедитесь, какой файл ак-

[42] KeePassDX на GitHub, лицензия GPL-3.0, основные функции бесплатны, рекомендуемая установка через F-Droid, на англ. Проверено: 2026-10-13.

[43] KeePassium на GitHub, лицензия GPLv3, бесплатно, платная подписка необязательна, на англ. Проверено: 2026-10-13.

[44] KeePassDX Wiki: AutoFill, пути в настройках приложения и выбор службы в Android, на англ. Проверено: 2026-10-13.

[45] KeePassium: настройка AutoFill на iOS, шаги описаны по iOS 17, подписи могут отличаться, на англ. Проверено: 2026-10-13.

туален. И помните: синхронизация не заменяет резервную копию. Удалённая или испорченная запись уедет на второе устройство так же, как и правка, поэтому отдельные проверенные копии из раздела выше остаются в силе.

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

Максимум

Дополнительно: ключи доступа. Ключи доступа (passkeys) KeePassXC хранит с версии 2.7.7:[a] для этого нужны программа на компьютере и расширение KeePassXC-Browser в браузере. По состоянию на март 2024 поддержка неполная: на некоторых сайтах создать или использовать такой ключ не получится.[b]

[a] KeePassXC: релиз 2.7.7 (запись от 10 марта 2024, поддержка Passkeys) и KeePassXC: релизы на GitHub («Browser: Add support for PassKeys»), на англ. Проверено: 2026-10-12.

[b] KeePassXC, issue 10374, ответ мейнтейнера от 10 марта 2024: поддержка passkeys ещё не полная; issue остаётся открытым, на англ. Проверено: 2026-10-13.

Максимум

Дополнительно: Bitwarden. Берите, если не хотите возиться с файлом и синхронизацией: есть другой проверенный вариант с открытым кодом — Bitwarden: основной код его приложений (GPL-3.0) и сервера (AGPL-3.0) открыт (часть кода лежит под отдельной лицензией Bitwarden),[a] независимые аудиты проводятся регулярно.[b] Ваше хранилище при этом лежит на сервере сервиса в зашифрованном виде, а не только у вас. Есть и платные облачные менеджеры паролей с закрытым кодом: здесь они не разбираются, в этой теме советуются только программы с открытым кодом.

[a] Репозитории bitwarden/clients (GPL-3.0) и bitwarden/server (AGPL-3.0); в корне bitwarden/clients также лежит файл LICENSE_BITWARDEN.txt (часть

кода под лицензией Bitwarden), на англ. Проверено: 2026-10-13.
[b]Bitwarden: независимые аудиты, на англ. Проверено: 2026-10-11.

Максимум

Дополнительно: вход по отпечатку. Вопреки совету выше, если приложение умеет открывать базу по отпечатку пальца, это можно включить для удобства, но мастер-пароль всё равно нужно помнить.

Максимум

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`.

Перенести остальные сайты

Почта уже переехала — самая опасная дыра закрыта. Дальше — пять важных сайтов за пять дней, по одному в день: банк, облако с фотографиями, мессенджеры, соцсети, магазин с привязанной картой. *(вывод автора)*

1. В первый день возьмите банк, во второй — облако с фотографиями и так далее по списку.
2. Смените пароль на сайте на сгенерированный так же, как для почты: генератор, сохранение в базу, выход и вход с новым паролем.
3. Отметьте сайт в записи: в поле `Notes` / `Заметки` укажите сегодняшнюю дату.

Получилось — когда для каждого из пяти сайтов в базе лежит свежий пароль.

Максимум

Дополнительно: остальные сайты. Всё, что не вошло в список, переносите по одному сайту за раз, каждый раз, когда вы всё равно заходите на него: меняйте пароль на сгенерированный и сохраняйте запись в базу тем же способом, что отработали на почте. Графика и дедлайна на весь список нет: забытый форум про рыбалку можно списать в отставку и не считать долгом.

Удалить пароль из 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.

Если вы никогда не отправляли пароль в переписке, пропустите этот раздел.

1. Смените пароль, который отправлялся в переписке, так же, как для почты: шаги — в разделах «Начать перенос с почты» и «Придумать пароль для сайта». Удаление сообщения пароль не отзывает.
2. Откройте последнюю переписку, где вы отправляли пароль, и попробуйте удалить сообщение у себя и у собеседника. Если сервис не позволяет удалить его у собеседника, удалите хотя бы у себя: пароль уже заменён.

Получилось — когда пароль из переписки заменён новым, а сообщение удалено у вас (и у собеседника, если сервис это позволил).

Передать пароль человеку

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, часто попадают 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 при личной встрече: не нужно создавать ссылку или оставлять сообщение. Телефонный звонок и голосовое сообщение для этого не годятся: разговор могут подслушать или записать, а голос и номер собеседника — подделать. Если встреча невозможна — почта, разные города, мастер, к которому неудобно подходить каждый раз, — не отправляйте пароль текстом напрямую, а воспользуйтесь сайтом **pass.yasno.club**: он показывает пароль получателю один раз и потом сам его удаляет. Это развёрнутый экземпляр open-source проекта Yopass. Ни один способ не даёт абсолютной тайны: получатель всё ещё может сфотографировать экран, пересказать пароль или сохранить его другим способом.

Если вы отправляете пароль.

1. Не отправляйте сразу в ответ на просьбу в чате: аккаунт собеседника могли взломать. Подождите до часа: тому, кому доступ нужен на самом деле, пароль нужен, и он перезапросит сам. Если повтора нет — позвоните собеседнику по номеру, который у вас уже был записан, и уточните просьбу. *(вывод автора)*
2. Откройте pass.yasno.club. Вставьте пароль в поле «Ваш секрет», в блоке «Будет удалён автоматически через» выберите «1 час», включите галочку «Одноразовая загрузка» и нажмите «Зашифровать».[46] Сайт покажет ссылку: она открывается один раз.

[46] pass.yasno.club, русский интерфейс страницы создания секрета: «Ваш секрет», «Будет удалён автоматически через», «1 час», «Одноразовая загрузка», «Зашифровать». Проверено: 2026-10-13.

3. Предупредите получателя, что ссылка **ОДНОРАЗОВАЯ**: напишите это рядом со ссылкой и скажите вслух, лично или по звонку (сам пароль по телефону не называйте): «Ссылка одноразовая: откройте её сразу, когда будете готовы записать пароль, и никому не пересылайте». Пусть не открывает «просто посмотреть».
4. Логин и пароль отправляйте **РАЗНЫМИ** каналами. Например, логин в мессенджере, а ссылку с паролем по почте или в другом мессенджере. Если один канал перехватят, одного логина или одного пароля для входа мало.
5. После передачи смените пароль: он больше не должен оставаться действующим после того, как необходимость закончилась.

Если вам прислали ссылку. Ссылка **ОДНОРАЗОВАЯ**: откройте её, только когда готовы сразу сохранить пароль, например в менеджер паролей. Не обновляйте страницу и не открывайте её дважды: второй раз пароля там уже не будет. Если ссылка не открывается, значит, её уже открыл кто-то другой или вышел срок. Сообщите отправителю: он создаст новую ссылку и сменит пароль.

Максимум

Дополнительно (на выбор): другие способы передать пароль. Выбирайте, когда нужен конкретный сервис, привычный получателю, или передача нужна внутри мессенджера. Специальные сайты для одноразовой передачи — это отдельные сервисы: каждый создаёт одну ссылку, показывает секрет один раз и сам её убивает. Ссылка во всех случаях должна быть строго **ОДНОРАЗОВАЯ**: после первого открытия пароль на сайте исчезает. После разовой передачи смените пароль, как в основном способе.

- **Bitwarden Send:** создайте одноразовую ссылку по официальной документации Bitwarden Send и задайте срок её действия. При необходимости защитите её паролем.[a] Подробнее об аудите: официальная страница Bitwarden.
- **Собственный пароль на ссылку в pass.yasno.club:** в

том же окне заполните поле «Собственный пароль»;[b] этот второй пароль передавайте другим каналом, чем ссылку.

- **Секретные чаты Telegram:** в профиле собеседника (меню «Ещё») 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. Секретные чаты доступны в мобильных приложениях. Это отдельная опция: включать её нужно каждый раз заново и на каждом устройстве, обычные чаты Telegram сами в секретные не превращаются.
- **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 share.yopass.se — публичной демо-версии открытого проекта Yopass с шифрованием OpenPGP на стороне браузера ещё до отправки на сервер, одноразовым просмотром и сроком жизни 1 час, 1 день или 1 неделя. Для по-настоящему чувствительных данных сам проект советует разворачивать Yopass у себя, а не полагаться на публичный демо-сервер.
- **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 номеру телефона или почте. 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.

[a] Bitwarden Send, срок действия, лимит доступов и пароль, на англ. Проверено: 2026-10-11.

[b] pass.yasno.club, русский интерфейс: поле «Собственный пароль». Проверено: 2026-10-13.

Максимум

Дополнительно: постоянный доступ нескольким людям. Там, где доступ нужен нескольким людям на постоянной основе — стриминг, семейный тариф, — отдавать свой личный пароль не лучший вариант, даже самым надёжным способом. У многих сервисов 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

Дополнительно: общая база. 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; при конфликте побеждает запись с более поздним изменением, старая версия остаётся в истории записи.[a]

- ☐ Завести общую базу KeePassXC с близким человеком для паролей, которые нужны вам обоим, — например для администратора домашнего роутера.

[a] KeePassXC User Guide, раздел о слиянии баз, на англ. Проверено: 2026-10-11.

Мастеру и гостям давайте пароль гостевой сети Wi-Fi, а не основной. Если на роутере гостевой сети нет, назовите основной пароль и смените его после визита. *(вывод автора)*

Максимум

Дополнительно: настроить гостевую сеть. Если ваш роутер умеет гостевую сеть (обычно это пункт «Гостевая сеть» в настройках Wi-Fi), заведите её заранее. Нет такого пункта — не страшно: основной совет остаётся прежним.

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 при личной встрече.
5. Отправить исчезающим сообщением, которое сотрётся через минуту.

Первые три. Дело не в мастере — дело в том, что сообщение может пережить 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 при личной встрече — бесплатно и надёжнее всего. Исчезаю-

щее сообщение — компромисс для случая, когда встретиться никак. Звонок по телефону не замена встрече: его могут подслушать, записать или подменить голос и номер. А основной пароль от Wi-Fi, если вы его назвали, 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.[47] 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 по нему одному не получится — если только вы сами не отдадите им и код.

Сделай это прямо сейчас

- ☐ Поставить на телефон 2FAS и включить резервную копию — 8 минут
- ☐ 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

[47] Credential stuffing — OWASP Community, на англ. Проверено: 2026-10-13.

Установить приложение для кодов

Приложение-генератор показывает числовой код и меняет его каждые 30 секунд (у части сервисов число цифр и шаг другие);[48] в настройках сервисов такой код обычно подписан словом TOTP. Считает его сам телефон — интернет для этого не нужен вовсе.

Берите 2FAS: код приложения открыт (лицензия GPLv3),[49] оно бесплатное, а из трёх сравниваемых приложений (2FAS, Aegis, Ente Auth) оно самое распространённое по числу установок.[50] Русского интерфейса у 2FAS нет,[51] поэтому его кнопки ниже названы по-английски.

Android: 2FAS, из Google Play

1. Поставьте 2FAS из Google Play и откройте его. Пролистайте вводные экраны до главного экрана: на нём внизу справа кнопка «+».
2. Включите PIN: «Settings» ☒ «Security» ☒ «Enable PIN Code», выберите 6 цифр (случайные, не дату рождения и не номер телефона). Забытый PIN не восстановить.[52]
3. Сразу сохраните PIN в KeePassXC: `New Entry...` / `Создать запись...` -> `Title` / `Название` (`2FAS — PIN`) -> `Password` / `Пароль` (эти 6 цифр) -> `OK` / `OK` -> `Save` / `Сохранить`.
4. Включите резервную копию: «Settings» ☒ «2FAS Backup», включите синхронизацию с Google Drive, выберите свой аккаунт Google и разрешите доступ.[53] (☒ синхронизация с облаком).

[48] RFC 6238: TOTP, одноразовые пароли по времени, на англ. Проверено: 2026-10-13.

[49] 2FAS Auth для Android: лицензия GPLv3 и 2FAS Auth для iOS: лицензия GPLv3, на англ. Проверено: 2026-10-13.

[50] 2FAS в Google Play (5 млн+ установок против 1 млн+ у Aegis и 100 тыс.+ у Ente Auth) и 2FAS в App Store (цена 0; около 35 тыс. оценок против менее 300 у Ente Auth), на англ. Проверено: 2026-10-13 (числа даны на эту дату).

[51] 2FAS: языки приложения: в списке готовых переводов русского нет, на англ. Проверено: 2026-10-13.

[52] 2FAS Auth: учебник («Settings ☒ Security ☒ Enable PIN Code», 4 или 6 цифр; забытый PIN не восстановить), на англ. Проверено: 2026-10-13.

[53] 2FAS: как работает синхронизация Google Drive («2FAS Backup», только Android), на англ. Проверено: 2026-10-13.

5. Задайте копии пароль. В KeePassXC нажмите `New Entry...` / `Создать запись...`, назовите её `2FAS — пароль копии`, в поле `Password` / `Пароль` нажмите значок кубика, выключите кнопку «/ * + & ...» (подсказка «Спецсимволы»: 2FAS принимает не все спецсимволы),[54] поставьте `Length` / `Длина` 24, нажмите `Apply Password` / `Использовать пароль`, затем `OK` / `OK` и `Save` / `Сохранить`. После этого в «2FAS Backup» ⊠ «Synchronisation Settings» задайте этот пароль для копии. Пароль копии не потеряйте: 2FAS в справке просит его запомнить.[55] (⊠ файл копии с паролем).
6. Нажмите `Lock Database` / `Заблокировать базу`. Список кодов в 2FAS пока пустой — так и надо: первая запись появится на следующем шаге, вместе с почтой.

iPhone: 2FAS, из App Store

1. Поставьте 2FAS из App Store и откройте его. Пролистайте вводные экраны до главного экрана: на нём вверху справа кнопка «+».
2. Включите PIN: «Settings» ⊠ «Security» ⊠ «Enable PIN Code», выберите 6 цифр (случайные, не дату рождения и не номер телефона). Забытый PIN не восстановить.[56]
3. Сразу сохраните PIN в KeePassXC: `New Entry...` / `Создать запись...` -> `Title` / `Название` (`2FAS — PIN`) -> `Password` / `Пароль` (эти 6 цифр) -> `OK` / `OK` -> `Save` / `Сохранить`.
4. Включите резервную копию: «Settings» ⊠ «2FAS Backup» и проверьте, что синхронизация iCloud включена (по справке 2FAS она включается сама, если вы вошли в iCloud).[57] (⊠ синхронизация с облаком).

[54] 2FAS для iOS, исходный код правил пароля копии (ExportFileRules.swift) (допустимы буквы, цифры и часть спецсимволов; минимум 3 символа) и KeePassXC, окно генератора паролей (PasswordGeneratorWidget.ui) (кнопка спецсимволов «/ * + & ...»), на англ. Проверено: 2026-10-13.

[55] 2FAS: как работает синхронизация Google Drive («Synchronisation Settings», пароль копии как дополнительная защита), на англ. Проверено: 2026-10-13.

[56] 2FAS Auth: учебник («Settings ⊠ Security ⊠ Enable PIN Code», 4 или 6 цифр; забытый PIN не восстановить), на англ. Проверено: 2026-10-13.

[57] 2FAS: как работает синхронизация iCloud (включается сама при входе в iCloud; ручное включение — «Settings ⊠ 2FAS Backup»), на англ. Проверено: 2026-10-13.

5. Задайте копии пароль. В KeePassXC нажмите `New Entry...` / `Создать запись...`, назовите её `2FAS — пароль копии`, в поле `Password` / `Пароль` нажмите значок кубика, выключите кнопку «/ * + & ...» (подсказка «Спецсимволы»: 2FAS принимает не все спецсимволы),[58] поставьте `Length` / `Длина` 24, нажмите `Apply Password` / `Использовать пароль`, затем `OK` / `OK` и `Save` / `Сохранить`. После этого в «2FAS Backup» ☒ «Manage Backup» задайте этот пароль для копии. Потерянный пароль копии не вернуть, а без него копия бесполезна.[59] (☒ файл копии с паролем).
6. Нажмите `Lock Database` / `Заблокировать базу`. Список кодов в 2FAS пока пустой — так и надо: первая запись появится на следующем шаге, вместе с почтой.

Видео: 2FAS — 2FA backup, or how to restore an account with lost 2FA? https://www.youtube.com/watch?v=Erwoc1UorBo

2FAS — 2FA backup, or how to restore an account with lost 2FA? — ролик на английском от разработчиков 2FAS, подсказка к резервной копии кодов; интерфейс может отличаться от текущей версии.

- 0:42 — резервные коды от сервиса
- 1:12 — файл копии с паролем
- 1:38 — синхронизация с облаком

Если код потом не принимается, проверьте время на телефоне: Android — «Часы» ☒ «Ещё» ☒ «Настройки» ☒ «Изменить дату и время» ☒ «Автоматическое определение даты и времени»;[60] iPhone — «Настройки» ☒ «Основные» ☒ «Дата и время» и включите автоматическую установку времени.[61] Код считается по времени, и сбитые часы дают код, который сервис отвергает; допустимое

[58] 2FAS для iOS, исходный код правил пароля копии (ExportFileRules.swift) (допустимы буквы, цифры и часть спецсимволов; минимум 3 символа) и KeePassXC, окно генератора паролей (PasswordGeneratorWidget.ui) (кнопка спецсимволов «/ * + & ...»), на англ. Проверено: 2026-10-13.

[59] 2FAS: как работает синхронизация iCloud («Manage Backup», дополнительный пароль копии, без него копию не восстановить), на англ. Проверено: 2026-10-13.

[60] Справка Android: дата и время. Проверено: 2026-10-13.

[61] Руководство пользователя iPhone: изменение даты и времени. Проверено: 2026-10-13.

расхождение обычно — не больше одного шага, около 30 секунд.[62]

Если на iPhone выключена «Связка ключей iCloud», копия 2FAS не восстановится: ключи шифрования копии хранятся в ней, а при выключенной связке 2FAS просит экспортировать ключи вручную («Manage Backup»).[63]

Если у сервиса варианта с приложением нет вовсе — включайте смс и не думайте: смс-код слабее приложения, но заметно лучше, чем ничего: в исследовании Google он остановил 100% автоматических атак, 96% массового фишинга и 76% целевых атак.[64] Номер иногда удаётся увести на чужую сим-карту, поэтому при возможности берите приложение.

Получилось — когда 2FAS открывается с PIN-кодом, в «2FAS Backup» синхронизация включена, а список кодов пуст. Так и должно быть: первый код появится на следующем шаге, когда вы добавите туда почту.

Максимум

Дополнительно (на выбор): другое приложение вместо 2FAS. Выбирайте по критерию, а не по вкусу:

- **Aegis Authenticator (только Android)** — если нужен русский интерфейс и хранилище, закрытое паролем. Бесплатный и открытый:[a] из Google Play или из F-Droid, если на телефоне нет Google Play. При первом запуске на экране `Security` / `Безопасность` выберите `Password` / `Пароль` (вариант `None` / `Нет` не выбирайте), пароль сгенерируйте в KeePassXC и сохраните в базу. Забытый пароль навсегда закроет коды.[b] Копия: `Settings` / `Настройки` -> `Backups` / `Резервные копии`.[c]

[62] RFC 6238: TOTP, одноразовые пароли по времени, на англ. Проверено: 2026-10-13.

[63] 2FAS для iOS, строки интерфейса (Localizable.strings): «iCloud Sync stores encryption keys in iCloud Keychain», на англ. Проверено: 2026-10-13.

[64] Google Security Blog: как эффективны базовые подсказки аккаунта (2019, Google, NYU, UCSD), на англ. Проверено: 2026-10-13.

- **Ente Auth (iPhone и Android)** — если нужны одни и те же коды на нескольких устройствах: в аккаунте Ente они хранятся со сквозным шифрованием, а без аккаунта работает кнопка «Use without backups».[d] Приложение открытое, в App Store бесплатное: Ente Auth.
- **Google Authenticator** — приложение Google, его код закрыт;[e] выбирайте, если хотите хранить коды в аккаунте Google.[f]

---

[a] Aegis Authenticator, официальный сайт, на англ. Проверено: 2026-10-13.

[b] Тексты интерфейса Aegis, русский перевод (strings.xml) («Безопасность», «Нет», «Пароль», предупреждение о потере пароля). Проверено: 2026-10-13.

[c] Тексты интерфейса Aegis, русский перевод (strings.xml) («Резервные копии», «Автоматическое резервирование хранилища»). Проверено: 2026-10-13.

[d] Ente Auth: частые вопросы («Use without backups», сквозное шифрование кодов в аккаунте, открытый код приложений), на англ. Проверено: 2026-10-13.

[e] Google Authenticator для Android на GitHub: открыт только устаревший форк, официальная версия остаётся закрытой, на англ. Проверено: 2026-10-13.

[f] Справка Google: приложение Google Authenticator: коды можно сохранять в аккаунте Google. Проверено: 2026-10-13.

Максимум

Дополнительно: аппаратный ключ. Выбирайте, если боитесь поддельных сайтов больше всего. 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 (ключ привязан к адресу сайта).[a] 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.

[a] Web Authentication Level 3, W3C (учётные данные доступны только сайтам своей организации-получателя; проверка адреса сайта: раздел «Validating the origin of a credential»), на англ. Проверено: 2026-10-13.

Максимум

Дополнительно (на выбор): коды в KeePassXC вместо приложения. Берите, если хотите держать коды на компьютере. 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, на разных защищённых носителях. 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`. (настроить TOTP).
3. В поле `Secret Key` / `Секретный ключ` вставьте только Base32-секрет. Не вставляйте целиком `otpauth://` URI.
4. Оставьте `Default settings (RFC 6238)` / `Параметры по умолчанию (RFC 6238)`, если сервис не сообщил другие параметры. При нестандартных настройках проверьте `Algorithm` / `Алгоритм`, `Time step` / `Временной шаг` 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 дождитесь автоочистки буфера обмена. (⊠ показать TOTP).

Системные часы компьютера и телефона должны быть точными: TOTP зависит от времени, и если часы устройства заметно сбились (допустимое расхождение обычно — не больше одного шага, около 30 секунд), код не примут.[a]

Видео: TroubleChute — KeePassXC TOTP (2-Factor Autofill) | Complete Crash Course https://www.youtube.com/watch?v=VEfkt29moE8

TroubleChute — KeePassXC TOTP (2-Factor Autofill) | Complete Crash Course — ролик на английском, подсказка только к пунктам меню: он показывает, как настроить и показать TOTP в KeePassXC. Делайте это в отдельном файле базы, как описано выше.

- 3:00 — настроить TOTP по секретному ключу
- 4:52 — показать TOTP

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 приложения для кодов 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 приложении, 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.

[a] RFC 6238: TOTP, одноразовые пароли по времени, на англ. Проверено: 2026-10-13.

Максимум

Дополнительно: перенести одну запись из Aegis в KeePassXC. Берите, если вы выбрали Aegis, а коды нужны ещё и в KeePassXC. В KeePassXC нет готового импорта из Aegis. 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 в файл`.
2. Выберите формат Text file (.TXT): в нём лежат `otpauth://` ссылки без шифрования, поэтому обращайтесь с файлом как с паролем. Зашифрованный JSON для ручного копирования секрета не подходит.[a]
3. Найдите в файле нужную запись и возьмите из её `otpauth://` ссылки только Base32-значение после `secret=`. QR-код и всю ссылку в KeePassXC не переносите и нигде не публикуйте. Файл с экспортом удалите после проверки, описанной под шагами.
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` / `Импорт 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 файл экспорта, кор-

зину и временные копии.

[a] Aegis, тексты интерфейса (strings.xml) («Import & Export», «Export», «Import from file», формат «Text file (.TXT)») и Aegis, код экспорта (ImportExportPreferencesFragment.java) (для текстового формата шифрование выключено и требуется подтверждение), на англ. Проверено: 2026-10-13.

Включить 2FA в почте

Начинать стоит с почты: через неё обычно приходят письма для восстановления пароля к другим сервисам, поэтому тот, кто получил доступ к почте, часто может захватить и их — и тогда другие замки уже мало что значат. *(вывод автора)* Ниже шаги для Gmail и Google-аккаунта; другая почта — в блоке «Дополнительно» после списка.

Почта: Gmail и Google-аккаунт, с компьютера

1. Откройте myaccount.google.com — в браузере, где уже открыта почта; заново входить не придётся.
2. Нажмите «Безопасность и вход в аккаунт».[65]
3. В разделе «Вход в Google» выберите «Включить двухэтапную аутентификацию» и пройдите шаги Google, указав свой номер телефона: смс-код станет запасным способом. Если двухэтапная аутентификация уже включена, этот пункт называется «Двухэтапная аутентификация» — откройте его.[66]
4. На странице «Двухэтапная аутентификация» нажмите «Настроить Authenticator» (на некоторых устройствах сначала «Начать»).[67]

[65] Справка Google: резервные коды и Справка Google: изменить пароль: раздел назван «Безопасность и вход в аккаунт» (в английской справке — Security & sign-in; на русской странице про включение двухэтапной аутентификации он назван короче, «Безопасность и вход»). Проверено: 2026-10-13.

[66] Справка Google: включить двухэтапную аутентификацию («Вход в Google» ⊠ «Включить двухэтапную аутентификацию») и Справка Google: резервные коды («Вход в Google» ⊠ «Двухэтапная аутентификация»). Проверено: 2026-10-13.

[67] Справка Google: приложение Authenticator для двухэтапной аутентификации: «Настроить Authenticator», на некоторых устройствах «Начать». Проверено: 2026-10-13.

5. Когда Google покажет QR-код, откройте 2FAS, нажмите «+» ⊠ «Scan a QR Code» и наведите камеру на экран.[68] Введите на странице Google код, который показывает 2FAS.
6. На странице «Двухэтапная аутентификация» найдите «Резервные коды», нажмите стрелку справа и выберите «Получить резервные коды». Их десять, каждый восьмизначный и срабатывает ровно один раз.[69] Вкладку не закрывайте: коды понадобятся на последнем шаге чек-листа.

Официально: как включить двухэтапную аутентификацию и про резервные коды.

Если Google не показывает «Настроить Authenticator», вернитесь на шаг 3 и убедитесь, что двухэтапная аутентификация действительно включена. *(вывод автора)*

Получилось — когда в разделе «Двухэтапная аутентификация» статус показывает, что она включена, а при следующем входе с нового устройства почта спрашивает не только пароль.

Максимум

Дополнительно (на выбор): другие способы подтверждения в Google. Вместо кода из приложения или в дополнение к нему:

- **Уведомления от Google** — если не хотите вводить код: на телефоне нажимаете «Да». Google советует их, если у вас нет ключа доступа: так проще, чем вводить код, и они защищают от подмены сим-карты.[a]
- **Ключ доступа** — если хотите входить отпечатком, лицом или PIN-кодом экрана; при входе с ключом второй этап пропускается.[b]

[a] Справка Google: включить двухэтапную аутентификацию: уведомления от Google рекомендованы при отсутствии ключа доступа, проще ввода кода

[68] 2FAS Auth: учебник (кнопка «+»: на Android внизу справа, на iOS вверху справа; «Scan a QR Code»), на англ. Проверено: 2026-10-13.

[69] Справка Google: резервные коды: набор из 10 кодов, 8 цифр, каждый одноразовый. Проверено: 2026-10-13.

и защищают от подмены сим-карты. Проверено: 2026-10-13.

[b]Справка Google: включить двухэтапную аутентификацию: при входе с ключом доступа второй этап пропускается. Проверено: 2026-10-13.

Максимум

Дополнительно: другая почта. В других почтовых сервисах обычно есть раздел «Безопасность» или «Вход и безопасность»; если не нашли — введите в поиске по настройкам «безопасность» или «двухфакторная». Дальше те же шаги: сначала приложение, смс запасным, затем резервные коды. *(вывод автора)*

Включить 2FA в Telegram

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.[70] Поэтому в русском интерфейсе он и называется «Облачным паролем»: искать его в настройках стоит по слову «пароль», а не «фактор».[71] Мессенджер идёт сразу после почты: там завязаны переписка и контакты. (☒ настройка облачного пароля). Правила выбора канала и запрет на отправку секретов разобраны в разделе «Выбрать защищённую связь».

Облачный пароль спрашивается на новом устройстве — и при входе по коду, и после того, как вы отсканировали QR-код своим телефоном. Ещё мошенники встраивают QR в «голосования» и «проверки»: отсканировав такой код, вы сами подтверждаете вход на устройстве мошенника.[72] Сканируйте QR, только когда сами вхо-

[70]Telegram FAQ: двухэтапная проверка, на англ. Проверено: 2026-10-13.

[71]Русский перевод интерфейса Telegram для Android, translations.telegram.org. Проверено: 2026-10-13.

[72]Пересказ в Bitdefender: схема с QR-кодом Telegram (QR выдают за «голосование» или «проверку»; сканирование открывает сессию мошенника, пароль не запрашивается), на англ. Проверено: 2026-10-13.

дите в Telegram на своём компьютере, и вводите облачный пароль только там.*(вывод автора)*

Telegram на Android и iPhone: «Облачный пароль»

1. Откройте Telegram: `Settings` / `Настройки` ⊠ «Конфиденциальность» ⊠ «Облачный пароль».[73]
2. Нажмите «Установить дополнительный пароль» (на iPhone — «Установить пароль»).[74]
3. Сгенерируйте пароль в KeePassXC по короткому сценарию записи (оценка не ниже `128 bit`): новый, не тот же, что от почты. Запись назовите `Telegram — облачный пароль`, затем нажмите `OK` / `OK`, `Save` / `Сохранить` и `Lock Database` / `Заблокировать базу`. Введите пароль в Telegram и повторите его.
4. Подсказку к паролю не вписывайте — пропустите этот шаг: подсказка видна тому, кто вводит пароль, и помогает подобрать его.*(вывод автора)*
5. Укажите резервную почту — свою, ту, где вы только что включили второй фактор: если облачный пароль забудется, вернуть доступ поможет именно она.[75]
6. Подтвердите почту: Telegram пришлёт письмо (проверьте и папку «Спам»), затем нажмите «Готово».[76]

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

Если Telegram не принял сгенерированный пароль, уберите из него спецсимволы (кнопка «/ * + & …» в генераторе) и сгенерируйте заново. *(вывод автора)*

Видео: Tech Talk — Как обезопасить Telegram | Полный Гайд https:

[73]Telegram FAQ: двухэтапная проверка (Settings > Privacy and Security > 2-Step Verification) и русский перевод интерфейса Telegram для Android («Конфиденциальность», «Облачный пароль»), на англ. Проверено: 2026-10-13.

[74]Русский перевод интерфейса Telegram для Android («Установить дополнительный пароль») и для iOS («Установить пароль»). Проверено: 2026-10-13.

[75]Telegram FAQ: двухэтапная проверка, на англ. Проверено: 2026-10-13.

[76]Русский перевод интерфейса Telegram для Android, translations.telegram.org («проверьте почту (не забудьте о папке со спамом)», «Готово»). Проверено: 2026-10-13.

//www.youtube.com/watch?v=_TjEEv-Inro

Tech Talk — Как обезопасить Telegram | Полный Гайд — 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

Раз в месяц и сразу после каждой смены телефона открывайте «Настройки» ☒ «Устройства» и завершайте незнакомые сеансы;[77] (☒ где открыть список сеансов). *(вывод автора)*

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

> **Максимум**
>
> **Дополнительно: код-пароль на само приложение.** Берите, если телефон иногда остаётся в чужих руках разблокированным. Откройте «Настройки» ☒ «Конфиденциальность» ☒ «Код-пароль» (на iPhone — «Код-пароль и Face ID» или «Код-пароль и Touch ID»), включите код-пароль («Включить код-пароль») и поставьте автоблокировку через 1 час.[a]
>
> [a] Русский перевод интерфейса Telegram для Android («Код-пароль», «Включить код-пароль», «Автоблокировка») и для iOS («Код-пароль и Face ID», «Через один час»). Проверено: 2026-10-13.

Включить 2FA в WhatsApp

В WhatsApp это отдельный секрет (раньше PIN, в августе 2026 года WhatsApp сообщил, что заменил его полноценным паролем),[78] который защищает перенос аккаунта на новый телефон. Он не заменяет код из SMS, а добавляет к нему ещё один секрет, который

[77] Telegram FAQ: Settings > Devices, на англ. Проверено: 2026-10-13.

[78] WhatsApp Blog: защита аккаунта, пароль вместо PIN (25.08.2026), на англ. Проверено: 2026-10-13.

мошеннику придётся узнать отдельно.

WhatsApp на Android и iPhone: двухшаговая проверка

1. Откройте WhatsApp: Android — три точки ⊠ «Настройки» ⊠ «Аккаунт» ⊠ «Двухшаговая проверка»; iPhone — «Настройки» ⊠ «Аккаунт» ⊠ «Двухшаговая проверка».[79]
2. Нажмите кнопку включения (по описанию до 25.08.2026 — «Enable» на Android, «Turn on» на iPhone; после перехода с PIN на пароль подпись могла измениться) и задайте пароль.[80]
3. Сгенерируйте пароль в KeePassXC по короткому сценарию записи (оценка не ниже `128 bit`), запись назовите `WhatsApp — двухшаговая проверка`, затем нажмите `OK` / `OK`, `Save` / `Сохранить` и `Lock Database` / `Заблокировать базу`. Введите пароль в WhatsApp и повторите его. Не храните его рядом с паролем от самого аккаунта.
4. Почту для восстановления добавьте — ту же, где включён второй фактор — и подтвердите её кодом из письма.[81] WhatsApp считает этот шаг необязательным; совет добавить её — *(вывод автора)*

Если WhatsApp не принял сгенерированный пароль, уберите из него спецсимволы и сгенерируйте заново; если не принял и этого — сократите длину, но не меньше 12 символов. *(вывод автора)*

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

Сохранить резервные коды

Резервные коды сохраняем только для почты Google: для Telegram и WhatsApp вы уже указали резервную почту, через неё возвраща-

[79] WhatsApp Help Center: о двухшаговой проверке (Settings > Account > Two-step verification; страница целиком не открылась, путь взят из выдачи поиска) и пересказ в Malwarebytes, на англ. Проверено: 2026-10-13.

[80] Пересказ в Malwarebytes: как включить двухшаговую проверку в WhatsApp («Enable» на Android, «Turn on» на iPhone; описание до замены PIN паролем), на англ. Проверено: 2026-10-13.

[81] Пересказ в Malwarebytes: как включить двухшаговую проверку в WhatsApp (почта для восстановления и код из письма), на англ. Проверено: 2026-10-13.

ют доступ. *(вывод автора)* Число и вид кодов у разных сервисов разные; у Google их десять, а новый набор выпускают в разделе «Резервные коды»[82] — 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 Google откройте «Двухэтапная аутентификация» -> «Резервные коды» -> «Получить резервные коды». Не закрывайте экран, пока запись не проверена. (☒ резервные коды от сервиса).
2. Откройте базу KeePassXC и откройте меню «Группы» и нажмите `New Group...` / `Создать группу...`, задайте имя группы `Двухфакторная аутентификация`.
3. В этой группе нажмите `New Entry...` / `Создать запись...` (откроется окно «Добавить запись») и создайте отдельную запись, не смешивая её с записью пароля аккаунта.
4. Заполните поля: `Title` / `Название`: `Google — резервные коды — личная почта`; `Username` / `Логин`: 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 дождитесь, пока KeePassXC сам очистит 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 дождитесь автоочистки буфера обмена. После успешного входа удалите только использованный код из `Notes` /

[82] Справка Google: резервные коды. Проверено: 2026-10-13.

Заметки, нажмите Save / Сохранить и заблокируйте базу через Lock Database / Заблокировать базу. 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, дождитесь автоочистки буфера обмена и заблокируйте базу через Lock Database / Заблокировать базу.

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

Цена второго фактора — несколько секунд на новом устройстве или после выхода из аккаунта: открыть приложение, подсмотреть код, ввести; на уже вошедшем устройстве код обычно не спрашивают, пока сессия активна. *(вывод автора)*

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» — одна из самых нажимаемых кнопок, 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

Почему нельзя откладывать обновления

Заплатка не только чинит дыру — она же и объявляет всему миру, что дыра там была. Вместе с обновлением крупные производители обычно публикуют открытый список исправлений: что именно исправлено и в каких версиях. С этого момента про уязвимость знают все — включая тех, кто автоматически ищет в интернете непропатченные устройства. Известные уязвимости, как правило, получают единый номер вида CVE-2026-12345. По нему в открытом каталоге cve.org находят краткое описание и ссылки на подробности, а оценку опасности — в базе NVD.

Получается парадокс: до выхода патча о дыре знал узкий круг — автор, производитель, иногда злоумышленники, — а сразу после выхода знает весь мир, и ваш телефон вдруг оказывается в списке тех самых непропатченных. *(вывод автора)* 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.

Какие дыры уже известны

Многие реально эксплуатируемые уязвимости давно закрыты производителем — месяцы и годы 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. Отсюда простое правило при покупке телефона: берите модель, которой производитель ещё выпускает обновления безопасности. Когда он перестаёт их выпускать, найденные позже дыры уже не закрываются, а известные остаются у вас. *(вывод автора)*

Базовый минимум при покупке телефона. Перед покупкой найдите срок обновлений именно этой модели (где искать — в списке ниже). Берите модель, которой обещано не меньше 5 лет обновлений безопасности. *(вывод автора)* Срок считается с выхода модели,

а не с вашей покупки (так у Google и Samsung, см. ниже). *(вывод автора)*

Где искать срок:

1. Google Pixel: справка Google. Pixel 8 и новее — 7 лет обновлений системы и безопасности, Pixel 6, 6a, 7, 7a и Pixel Fold — 5 лет, считая с даты, когда модель впервые появилась в Google Store в США; Pixel 5a и старше обновлений не получают.[83]
2. Samsung Galaxy: страница безопасности Samsung перечисляет модели, которые получают патчи каждый месяц и раз в квартал, и называет срок «до 7 лет», объявленный в январе 2024 года; для Galaxy S26 Samsung пишет «семь лет обновлений безопасности» от даты глобального запуска, сроки зависят от модели, оператора и рынка.[84]
3. Fairphone: для Fairphone 5 производитель гарантирует не меньше 8 лет программной поддержки.[85]
4. iPhone: Apple срок не называет. Откройте список выпусков безопасности Apple и найдите свою модель в столбце «Available for»: пока она там встречается в свежих выпусках, обновления безопасности для неё выходят. *(вывод автора)* Для старых моделей Apple выпускает отдельные обновления прежних версий iOS, например iOS 18.7.10 для iPhone XS, XS Max и XR.[86]
5. Телефон уже у вас: «Настройки» ☒ «О телефоне» ☒ «Версия

[83]Справка Google Pixel: сроки обновлений, для Pixel 8 и новее — 7 лет обновлений ОС и безопасности, отсчёт от первой доступности в Google Store в США, на англ. Проверено: 2026-10-13.

[84]Samsung Mobile Security: модели и частота патчей, «As of January 2024, we are extending our security update support for Samsung Galaxy devices by up to 7 years», списки «Monthly» и «Quarterly Security Updates»; Samsung: Galaxy S26 Series, «seven generations of OS upgrades and seven years of security updates» от даты глобального запуска; сроки зависят от модели, оператора и рынка, на англ. Проверено: 2026-10-25.

[85]Fairphone: Software longevity, «guaranteed software support for at least eight years, with five major Android updates» для Fairphone 5, на англ. Проверено: 2026-10-25.

[86]Apple: Security releases, столбец «Available for»; Apple не называет срока поддержки iPhone на этой странице; для старых моделей выходят отдельные выпуски, например iOS 18.7.10 для iPhone XS, XS Max, XR, на англ. Проверено: 2026-10-25.

Android» и строка «Обновление системы безопасности» с датой (названия на разных телефонах отличаются).[87] Если дата давно не менялась, откройте страницу производителя из пунктов выше: возможно, поддержка модели закончилась. *(вывод автора)*

По опубликованным обещаниям дольше всех поддерживают Fairphone 5 (не меньше 8 лет), затем Google Pixel 8 и новее и флагманы Samsung (до 7 лет); Apple срок не публикует, поэтому для iPhone берите модель из списка устройств, которые поддерживает актуальная версия iOS. *(вывод автора)*

Включить автообновление на телефоне

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

Базовый минимум.

Android: приложения и система

1. Приложения: откройте Google Play, нажмите на фото профиля в правом верхнем углу ⊠ `Settings` / `Настройки` ⊠ `Network preferences` / `Настройки подключения` ⊠ `Auto-update apps` / `Автообновление приложений` ⊠ «Обновление только через Wi-Fi». Это не тратит мобильный трафик, а на Wi-Fi телефон бывает регулярно.[88]
2. Система: откройте `Settings` / `Настройки` ⊠ «Система» ⊠ «Обновления ПО». Большинство системных обновлений Android ставит сам в фоне, а вступают они в силу после перезапуска; отдельного переключателя включать не нужно.[89]

[87] Справка Android: проверить и обновить версию Android, Settings ⊠ About phone ⊠ Android version, строка «Android security update», на англ. Проверено: 2026-10-25.

[88] Справка Google Play: автообновление приложений. Проверено: 2026-10-13.

[89] Справка Android: обновление системы, путь «Система» ⊠ «Обновления ПО», автоматическая установка и применение после перезапуска. Проверено: 2026-10-13.

3. Когда придёт уведомление об обновлении, откройте его и нажмите «Обновить» в тот же вечер: подключите телефон к Wi-Fi и зарядите минимум до 75 %.[90]

Если не нашли «Система» ⊠ «Обновления ПО» — введите слово «обновление» в строке поиска по настройкам. *(вывод автора)* Если обновление не скачалось — телефон повторит попытку в ближайшие несколько дней; не хватает места — смотрите раздел про отложенное обновление ниже.[91]

iPhone: приложения и система

1. Приложения: `Settings` / `Настройки` ⊠ «Приложения» ⊠ `App Store` ⊠ включите «Обновления приложений».[92]
2. Система: `Settings` / `Настройки` ⊠ «Основные» ⊠ «Обновление ПО» ⊠ «Автообновление» ⊠ включите «Устанавливать автоматически». Переключатель «Загружать автоматически» отдельно включать не нужно: он виден только при выключенной автоустановке.[93]
3. Дальше iPhone ставит обновление ночью, когда заряжается и подключён к Wi-Fi, а перед установкой присылает уведомление.[94]

Если утром в «Основные» ⊠ «Обновление ПО» всё ещё висит доступное обновление — ночью не было зарядки или Wi-Fi: поставьте его вручную по разделу про отложенное обновление ниже. *(вывод автора)*

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

[90] Справка Android: обновление системы, требование Wi-Fi и заряда не меньше 75 %. Проверено: 2026-10-13.

[91] Справка Android: обновление системы, повторная попытка скачивания в течение нескольких дней. Проверено: 2026-10-13.

[92] Apple: автоматические обновления приложений на iPhone, на англ. Проверено: 2026-10-13.

[93] Apple: автоматическое обновление iOS, «Устанавливать автоматически» и «Загружать автоматически». Проверено: 2026-10-13.

[94] Apple: автоматическое обновление iOS, ночная установка при зарядке и Wi-Fi, уведомление перед установкой. Проверено: 2026-10-13.

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

Максимум

Дополнительно (на выбор): другие варианты автообновления приложений в Google Play. В том же меню «Автообновление приложений» есть ещё три пункта.[a] «Обновление через Wi-Fi или мобильный интернет» берите, если почти не бываете на Wi-Fi и мобильный трафик не ограничен. «Обновление с ограниченным расходом трафика» — компромисс между двумя первыми, он доступен не всем пользователям. «Никогда» не выбирайте: это выключенное автообновление.

Дополнительно (на выбор): телефон не Pixel. Сроки выхода обновлений зависят от устройства, производителя и оператора связи; пункт «Система» ☒ «Обновления ПО» в справке Google описан для Android в целом, но если на вашем телефоне его нет, спросите у производителя.

[a] Справка Google Play: автообновление приложений, четыре варианта пункта «Автообновление приложений». Проверено: 2026-10-13.

Включить автообновление на компьютере

На компьютере всё зависит от системы: ниже по одному пути для Windows 11, Windows 10 и macOS, затем браузер.

Базовый минимум.

Windows 11: проверить, что обновления не на паузе

1. Откройте `Start` / `Пуск` ☒ `Settings` / `Параметры` ☒ «Центр обновления Windows».[95]
2. Windows 11 скачивает и ставит обновления сама, включать ничего не нужно. Смотрите на строку «Приостановить об-

[95] Microsoft: Windows Update FAQ, путь Start > Settings > Windows Update и пункт Pause updates; название кнопки возобновления на этой странице не указано, на англ. Проверено: 2026-10-13.

новления»: если пауза включена, нажмите на этом же экране «Возобновить обновления» (Resume updates) и дождитесь, пока Windows проверит и поставит обновления. *(вывод автора)*

С Windows 10 иначе: обычная поддержка закончилась 14 октября 2025 года, и обновления безопасности Windows 10 по обычной схеме больше не выходят.[96] Дальше — один путь, программа ESU на бесплатных условиях: она продлевает обновления безопасности.

Windows 10: бесплатная программа расширенных обновлений (ESU)

1. Проверьте версию: `Settings` / `Параметры` ⊠ «Система» ⊠ «О системе» ⊠ раздел «Характеристики Windows» и запомните номер версии.[97]
2. Для ESU нужна версия 22H2. Войдите в Windows учётной записью Microsoft с правами администратора, а не локальной и не детской: ESU работает только так.[98]
3. Откройте `Settings` / `Параметры` ⊠ «Обновление и безопасность» ⊠ «Центр обновления Windows» и нажмите «Enroll now» («Зарегистрироваться»).[99]
4. Выберите бесплатный способ — синхронизацию параметров компьютера (PC Settings sync) с учётной записью Microsoft.[100]
5. Готово: обновления безопасности будут приходить до 12 октября 2027 года.[101]

[96]Microsoft: поддержка Windows 10 закончилась 14 октября 2025, на англ. Проверено: 2026-10-13.

[97]Microsoft: какая версия Windows установлена, путь System > About, раздел Windows specifications, на англ. Проверено: 2026-10-13.

[98]Microsoft: расширенные обновления безопасности (ESU) для Windows 10, требования: Windows 10 22H2, учётная запись Microsoft администратора, не детская, на англ. Проверено: 2026-10-13.

[99]Microsoft: расширенные обновления безопасности (ESU) для Windows 10, путь Settings > Update & Security > Windows Update, кнопка «Enroll now», на англ. Проверено: 2026-10-13.

[100]Microsoft: расширенные обновления безопасности (ESU) для Windows 10, бесплатная регистрация через синхронизацию параметров, на англ. Проверено: 2026-10-13.

[101]Microsoft: расширенные обновления безопасности (ESU) для Windows 10, срок до 12 октября 2027, на англ. Проверено: 2026-10-13.

Нет кнопки «Enroll now» — сначала поставьте все доступные обновления в том же «Центре обновления Windows» и повторите шаг 3.[102] Не подошло и после этого — переходите к разделу «Понять, что устройство пора менять» ниже.

macOS: автоматические обновления

1. Откройте System Settings / Системные настройки ☒ «Основные» ☒ «Обновление ПО».
2. Нажмите кнопку «Информация» рядом с пунктом «Автоматические обновления» и включите три переключателя: «Download new updates when available», «Install macOS updates» и «Install Security Responses and system files» (так они названы в английской справке Apple). Нажмите «Готово».[103]
3. На ноутбуке адаптер питания должен быть подключён, иначе обновления не скачаются автоматически.[104]

Браузер. Основной путь — Chrome: он обновляется сам в фоне, но применяет новую версию только после перезапуска.

Chrome: проверить и применить обновление

1. Нажмите «Ещё» (три точки в правом верхнем углу) ☒ «Справка» ☒ «О браузере Google Chrome». Страница сама проверит наличие обновления.[105] (☒ проверка обновления)
2. Если есть кнопка «Перезапустить» — нажмите её, а не закрывайте окно вручную. Chrome откроет вкладки заново; окна инкогнито не восстанавливаются.[106] Кнопки нет — у вас уже последняя версия. (☒ обновление всех программ). (☒ список программ и удаление лишнего)

[102] Microsoft: расширенные обновления безопасности (ESU) для Windows 10, требование установить последние обновления Windows, на англ. Проверено: 2026-10-13.

[103] Apple: обновление macOS, путь System Settings > General > Software Update, три переключателя, питание ноутбука, на англ. Проверено: 2026-10-13.

[104] Apple: обновление macOS, питание ноутбука при автоматической загрузке, на англ. Проверено: 2026-10-13.

[105] Справка Chrome: обновление браузера, на англ. Проверено: 2026-10-13.

[106] Справка Chrome: обновление браузера, кнопка Relaunch, вкладки возвращаются, окна инкогнито нет, на англ. Проверено: 2026-10-13.

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

Максимум

Дополнительно (на выбор): Windows 10 — другие способы подключить ESU. Берите, если синхронизация параметров вам не подходит. Остальные способы: 1000 баллов Microsoft Rewards или разовый платёж 30 долларов США (или эквивалент в местной валюте) плюс налог. Одна лицензия покрывает до 10 устройств.[a]

Дополнительно (на выбор): Microsoft Edge. Берите, если пользуетесь Edge: «Настройки и прочее» (три точки) ⊠ «Справка и отзывы» ⊠ «О Microsoft Edge». Если пишет «To finish updating, restart Microsoft Edge» — нажмите «Restart» («Перезапустить»); если Edge предлагает скачать обновление — скачайте его. Edge по умолчанию обновляется сам при перезапуске.[b]

Дополнительно (на выбор): Firefox. Берите, если пользуетесь Firefox: в `Settings` / `Настройки` ⊠ «Основные» ⊠ «Обновления Firefox» есть вариант «Автоматически устанавливать обновления» (в английском интерфейсе Automatically install updates), его стоит один раз проверить. Новая версия, как и в Chrome, включается после перезапуска.[c]

[a] Microsoft: расширенные обновления безопасности (ESU) для Windows 10, 1000 баллов Rewards, разовый платёж 30 долларов США, до 10 устройств, на англ. Условия и цена могут меняться. Проверено: 2026-10-13.

[b] Microsoft: настройки обновления Edge, на англ. Проверено: 2026-10-13.

[c] Mozilla Support: Update Firefox to the latest release, на англ.; название варианта «Automatically install updates» подтверждено по описанию в результатах поиска, страница не отдала текст при прямом открытии. Проверено: 2026-10-13.

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

Установить отложенное обновление

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.

Базовый минимум.

Поставить отложенное обновление

1. Подключите телефон к зарядке и Wi-Fi (на Android заряд — минимум 75 %).[107]
2. Откройте раздел обновлений: на Android — `Settings` / `Настройки` ☒ «Система» ☒ «Обновления ПО», на iPhone — `Settings` / `Настройки` ☒ «Основные» ☒ «Обновление ПО» (то же, что в разделе про автообновление на телефоне). Следуйте инструкциям на экране.
3. Подтвердите перезапуск, когда попросит система, и оставьте телефон заряжаться — дальше он справится сам.

Типовой сбой — не хватает свободного места. Держите свободными не меньше 5 ГБ. *(вывод автора)* Точный объём зависит от версии обновления и в справках Apple и Google не указан. iPhone при нехватке места может сам временно удалить приложения и вернуть их после обновления.[108]

iPhone: освободить место перед обновлением

[107] Справка Android: обновление системы, заряд не меньше 75 % и Wi-Fi. Проверено: 2026-10-13.

[108] Apple: автоматическое обновление iOS, при нехватке места система может временно удалить приложения и переустановить их после обновления; точный объём на странице не указан. Проверено: 2026-10-13.

1. `Settings` / `Настройки` ⊠ «Основные» ⊠ «Хранилище iPhone» и включите «Выгружать неиспользуемые». Приложения удалятся, а их данные останутся, и при следующем запуске всё скачается заново.[109]

Android: освободить место перед обновлением

1. Откройте приложение Files by Google ⊠ вкладка «Очистка» и удалите то, что оно предложит: старые скриншоты, дубликаты, давно не открытые файлы. *(вывод автора)*

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

> **Максимум**
>
> **Дополнительно (на выбор): путь «Настройки» ⊠ «Хранилище» на Android.** Берите, если Files by Google нет на телефоне: у многих моделей там кнопка «Освободить место», путь зависит от производителя. *(вывод автора)*

Понять, что устройство пора менять

Бывает и так, что автообновление включать уже некому: производитель официально прекратил выпускать обновления для конкретной модели, и официальных патчей для неё больше не будет, сколько ни жди.

Базовый минимум.

1. Сегодня перенесите почту и банковские приложения на устройство, которое ещё получает обновления.
2. Старый телефон или ноутбук оставьте только для новостей и музыки: там цена ошибки заметно ниже.
3. Запланируйте замену — запишите дату в календарь не позже чем через 12 месяцев. *(вывод автора)*

[109] Apple: хранилище iPhone, путь Settings > General > iPhone Storage, переключатель Offload Unused Apps, на англ. Проверено: 2026-10-13.

Для компьютера на Windows 10 без ESU (или вообще любого старого железа, до которого обновления уже не доходят) порядок один:

Старый Windows-компьютер: Windows 11 или Linux Mint

1. Скачайте Microsoft PC Health Check — aka.ms/GetPCHealthCheckApp — установите и нажмите «Проверить сейчас». Приложение Windows 11 само не ставит, а сообщает, подходит ли компьютер.[110]
2. Подходит — обновитесь до Windows 11 бесплатно: когда Windows 11 станет доступна для вашего компьютера, Центр обновления Windows предложит её сам; нужна Windows 10 версии 2004 или новее.[111]
3. Не подходит — поставьте Linux Mint (Cinnamon): бесплатный, почти все пакеты — с открытым кодом, с рабочим столом, похожим на Windows. Скачайте с linuxmint.com/download.php и ставьте по руководству по установке.[112] Часть специфичного софта — отдельные банк-клиенты, некоторые игры — под Linux может не работать. *(вывод автора)*

> **Максимум**
>
> **Дополнительно (на выбор): ChromeOS Flex.** Берите, если вам нужен только браузер и почта. Бесплатный, от Google, превращает старый компьютер в подобие Chromebook. Официально поддерживается только на сертифицированных моделях.[a] Список — на support.google.com/chromeosflex, страница проекта — chromeos.google/products/chromeos-flex. Обычные десктопные программы на Flex в основном не запустятся; порядок выше (сначала Mint) — потому что Mint бесплатный и почти весь с открытым кодом. *(вывод автора)*

[110]Microsoft: системные требования Windows 11, приложение PC Health Check, на англ. Проверено: 2026-10-13.

[111]Microsoft: системные требования Windows 11, нужна Windows 10 версии 2004 или новее; ждать, пока Windows Update сообщит о готовности Windows 11, на англ. Проверено: 2026-10-13.

[112]Linux Mint: скачивание, издания Cinnamon, Xfce, MATE; Cinnamon названа самой популярной, на англ. Проверено: 2026-10-13.

Дополнительно (на выбор): включение TPM 2.0 и Secure Boot в BIOS. Берите, если PC Health Check отказал только из-за них: в BIOS компьютера нужно включить оба пункта, и приложение проверить повторно. Расположение пунктов зависит от производителя материнской платы.

Дополнительно (на выбор): сверить срок перед покупкой следующего телефона. 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.

[a] Google: ChromeOS Flex, бесплатный, официально поддерживается только на сертифицированных моделях, на англ. Проверено: 2026-10-13.

Максимум

Дополнительно (на выбор): роутер. Самая забытая железка в доме — роутер. Берите, если роутер куплен вами, а не выдан провайдером. Базовый порядок один: сначала приложение производителя; нет приложения — веб-интерфейс.

1. Приложение производителя. У TP-Link это Tether: «More» ⊠ «System» ⊠ «Firmware Update» (на роутерах с TP-Link Cloud).[a] У ASUS — ASUS Router: вкладка «Settings», пункт обновления прошивки и проверка версии.[b] У Keenetic справка описывает обновление через мобильное приложение.[c] На других роутерах ищите приложение производителя в документации к роутеру. *(вывод автора)*
2. Нет приложения — откройте веб-интерфейс по адресу из документации роутера. Например, у TP-Link это `tplin`

`kwifi.net`, раздел «Advanced» ⊠ «System» ⊠ «Firmware Upgrade» (для роутеров без TP-Link Cloud — загрузка файла прошивки).[d]

3. Роутер выдан провайдером и доступа к настройкам нет — напишите провайдеру с просьбой обновить прошивку. *(вывод автора)*
4. Пароль администратора: у TP-Link по умолчанию `admin` / `admin`.[e] Замените его на пароль, сгенерированный в KeePassXC с оценкой не ниже `128 bit` (как в теме про пароли), и сразу сохраните в базу. Раздел настроек с этим паролем у разных роутеров называется по-разному — ищите по слову «пароль». *(вывод автора)*

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

[a] TP-Link: как войти в веб-интерфейс роутера, Tether: More > System > Firmware Update, на англ. Проверено: 2026-10-13.

[b] ASUS: обновление прошивки роутера через приложение ASUS Router, на англ. Проверено: 2026-10-13.

[c] Keenetic: обновление KeeneticOS, справка описывает обновление через мобильное приложение, на англ. Проверено: 2026-10-13.

[d] TP-Link: как войти в веб-интерфейс роутера, адрес tplinkwifi.net, Advanced > System > Firmware Upgrade, на англ. Проверено: 2026-10-13.

[e] TP-Link: как войти в веб-интерфейс роутера, логин и пароль по умолчанию admin, на англ. Проверено: 2026-10-13.

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

Фишинг, поддельные сайты и сертификаты

Фишинг — одна из самых массовых атак, и целится она вовсе не в технику: антивирус и обновления от клика не спасут, потому что дверь в этой схеме открывает сам человек. Менеджер паролей поможет, только если не вставлять пароль вручную: на чужом домене он ничего не подставит. 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

- ☐ Входить в банк из закладки или из приложения банка, а в почту — из закладки — 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

Как работает обман

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 основные 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 в тексте письма фильтры проверяют, а адрес, зашитый в картинку-QR, многие из них не разбирают.

Базовый минимум.

1. Платите по QR только внутри приложения своего банка. Если адреса, куда ведёт код, нет в приложении, оплату не подтверждайте.
2. QR-код, который вы не ждали (наклейка на автомате, код в письме), не открывайте. Нужна услуга — зайдите на её сайт через свою закладку (как её сделать, описано в разделе «Заходить в банк и почту своим путём» ниже).

Результат: оплату по QR вы подтверждаете только внутри приложения банка, а ссылки из неожиданных кодов не открываете.

> **Максимум**
>
> **Дополнительно (на выбор): прочитать адрес из QR.** Берите, если код нужен для чего-то кроме оплаты — например, меню в кафе. Камера большинства телефонов показывает адрес из QR над кнопкой «Открыть» *(вывод автора)*: прочитайте его справа

> налево, как в разделе про адрес сайта, прежде чем нажимать. Адрес не показан или не похож на ожидаемый — не открывайте. Вместо чтения можно набрать известный адрес вручную.

Раскрыть ссылку до клика

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.

Базовый минимум.

Компьютер: навести курсор

1. Наведите курсор на ссылку или кнопку, не нажимая, — настоящий адрес появится внизу окна браузера[113] (в Safari на Mac сначала включите «Вид ☒ Показать строку состояния»). *(вывод автора)*
2. Прочитайте адрес справа налево (правило в следующем разделе).
3. Адрес не показан или не похож на ожидаемый — не нажимайте. Нужный сайт откройте через свою закладку.

Если не получилось. Строка с адресом не появилась — считайте ссылку непроверенной и откройте сайт через закладку.

Телефон: зажать ссылку пальцем

1. Нажмите на ссылку или кнопку и удерживайте палец, пока не появится меню действий или превью с адресом.
2. Прочитайте адрес справа налево. Не похож на ожидаемый — уберите палец, не выбирая ни один из пунктов.
3. Адрес не показан — ничего не нажимайте и откройте сайт через свою закладку.

Если не получилось. Кнопка в письме не раскрывается — это тот

[113] Справка Gmail: как сообщить о фишинге, на компьютере наведите указатель на ссылку и сверьте адрес. Проверено: 2026-10-13.

же случай: считайте ссылку непроверенной и откройте сайт через закладку. *(вывод автора)*

> **Максимум**
>
> **Дополнительно: скопировать адрес ссылки на компьютере.** Берите, если адрес длинный и внизу окна не читается целиком. Щёлкните по ссылке правой кнопкой и выберите пункт про копирование адреса ссылки (точные подписи в Chrome, Firefox, Safari и Edge не подтверждены, поэтому ищите пункт со словами «копировать» и «ссылка»), вставьте адрес в «Блокнот» (Windows) или TextEdit (Mac) и прочитайте его там. В адресную строку браузера вставлять не стоит: случайный Enter откроет ссылку.

Официально: как распознать фишинговое письмо, Google.

Прочитать адрес сайта

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 (`/`; а также перед `?` и `#`) и без порта (`:8080`), 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.au`, `.co.jp`)[114] — 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

[114] Public Suffix List, на англ. Проверено: 2026-10-12.

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: эта часть не адрес сайта (это логин для входа), поэтому вы окажетесь на том, что стоит 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 @, — не адрес сайта, 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 — его можно посмотреть в сведениях о письме.[115] Откройте в почте последнее письмо на тему вроде «подтвердите данные» — такое почти наверняка найдётся.

Базовый минимум.

1. Раскройте настоящий адрес отправителя способом ниже: Gmail, если у вас почта Gmail, и «Почта» на iPhone, если вы читаете письма ею.

[115] Проверка подлинности письма в Gmail, Справка Google. Проверено: 2026-10-12.

2. Прочитайте домен после @ справа налево, по сегментам через точку.
3. Домен не совпадает с сайтом банка — не отвечайте, не открывайте ссылки и вложения, письмо удалите. Если вопрос к банку остался, зайдите в приложение банка или позвоните по номеру из контактов «Банк» (раздел ниже).
4. Ваша почта — не Gmail и не «Почта» на iPhone: считайте такое письмо непроверенным и ссылки из него не открывайте. *(вывод автора)*

Gmail: раскрыть настоящий адрес отправителя

1. На компьютере откройте письмо и нажмите стрелку (вниз) у имени отправителя *(вывод автора)* — покажутся настоящий адрес и домены «отправлено через» и «подписано»: те, что письмо реально отправили и подписали.[116]
2. В приложении на телефоне откройте письмо, нажмите «Подробности» и затем «Смотреть параметры безопасности» — там те же сведения. Письмо проверено, если в «отправлено через» указан домен, а в «подписано» — домен отправителя.[117]
3. Знак вопроса рядом с именем отправителя — тревожный сигнал: сам Gmail не смог подтвердить подлинность письма.[118] Не нажимайте ссылки и вложения, затем на компьютере откройте письмо, нажмите «Ещё» рядом с кнопкой ответа и выберите «Сообщить о фишинге».[119]

Если не получилось. Нет строк «отправлено через» и «подписано» — письмо не проверено, считайте его подозрительным.

---

[116] Проверка подлинности письма в Gmail на компьютере, Справка Google, на англ. (стрелка вниз у имени отправителя, заголовки «Mailed by» и «Signed by»); русские подписи заголовков «отправлено через» и «подписано» взяты из русской версии той же справки. Проверено: 2026-10-13.

[117] Проверка подлинности письма в Gmail, Справка Google, «Подробности» ☒ «Смотреть параметры безопасности», заголовки «отправлено через» и «подписано». Проверено: 2026-10-13.

[118] Проверка подлинности письма в Gmail, Справка Google. Проверено: 2026-10-13.

[119] Справка Gmail: как сообщить о фишинге, на компьютере значок «Ещё» рядом с кнопкой ответа ☒ «Сообщить о фишинге»; для приложения на телефоне страница шагов не приводит. Проверено: 2026-10-13.

Официально: как проверить подлинность письма.

Почта на iPhone: раскрыть адрес отправителя

1. Откройте письмо и нажмите на имя отправителя в шапке — на экране откроется карточка с его настоящим адресом. *(вывод автора)*
2. Прочитайте адрес тем же способом, что и в ссылке, — справа налево.

Если не получилось. Карточка не открылась — считайте письмо непроверенным.

Получилось — когда вы нашли такое письмо, раскрыли настоящий адрес отправителя, прочитали его домен справа налево и знаете, что с ним делать: совпал с банком — продолжайте через приложение банка или закладку, не совпал — письмо удалено.

Заметить подмену в адресе

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 `vashbank.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 браузеры часто ловят такую подмену сами: если в одном слове адреса смешались буквы из разных алфавитов, браузер обычно показывает не красивую подделку, а её техническое имя — нечитаемую строку вида `xn`

--... — и подмена бросается в глаза без всякого чтения.[120] Не ловятся слова целиком из похожих букв другого алфавита (Chrome ловит такое не всегда, Firefox пропускает) и похожие буквы одного алфавита, например латинские `rn` вместо `m`: смешения алфавитов там нет, ловить браузеру нечего.[121] 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.

Что значит замочек в браузере

Замочек (в новых версиях Chrome — значок настроек слева от адреса) 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 бесплатно и автоматически, и это никак не связано с тем, кто и зачем сайт создал.[122]

Базовый минимум. Сам по себе значок замка этого не доказывает: он подтверждает шифрование соединения и владение указанным доменом, но не честность сайта. Вводите пароль и данные карты только на сайте, открытом из своей закладки или из приложения банка. Замочек и сходство адреса с настоящим не считайте поводом вводить данные. Пришлось открыть сайт не из закладки — прочитайте домен справа налево по правилам выше; домен не совпал с ожидаемым хоть в одном символе — закройте вкладку и

[120] Internationalized Domain Names (IDN) in Google Chrome, на англ. Проверено: 2026-10-11.

[121] IDN Display Algorithm, Mozilla Wiki (Firefox) и IDN в Google Chrome (Chrome), на англ. Проверено: 2026-10-12.

[122] Challenge Types, Let's Encrypt (проверяется только контроль над доменом, чаще всего автоматически) и About, Let's Encrypt (бесплатно и автоматически), оба на англ. Проверено: 2026-10-12.

зайдите через закладку.

Максимум

Замочек выдаёт удостоверяющий центр — организация, которая выпускает сертификаты и подписывает их своей подписью; эту подпись браузеры и устройства заранее внесли в список доверенных, поэтому проверяют её автоматически, без вашего участия. (☒ удостоверяющие центры и цепочка доверия). 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.[a] 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. (☒ корневой сертификат).

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 https://www.youtube.com/watch?v=EA9Y1rBaF-o

Tech Talk — Все об SSL-сертификатах — подсказка к сертификатам и замочку, а не полный курс по фишингу.

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

☐ Открыть сайт своего банка, нажать на значок слева от ад-

реса (замок или значок настроек) ⊠ «Подключение защищено» ⊠ «Действительный сертификат» и посмотреть, кому и кем выдан сертификат.

[a] Challenge Types, Let's Encrypt, на англ. Проверено: 2026-10-11.

Заходить в банк и почту своим путём

Одно правило закрывает основные варианты письма со ссылкой: в банк и почту заходим своим путём, 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.

Базовый минимум. В банк заходите из закладки в браузере или из приложения банка, в почту — из закладки.

1. Банк на телефоне: откройте приложение банка. Оно уже стоит на телефоне; если его нет, поставьте из официального магазина приложений (App Store или Google Play).
2. Почта и банк на компьютере: добавьте сайт в закладки. Откройте адрес, набрав его в строке браузера вручную один раз. Адрес почты вы знаете; адрес сайта банка возьмите с обратной стороны карты, а если его там нет — из договора с банком.
3. На компьютере добавьте страницу в закладки сочетанием `Ctrl+D` (Windows и Linux) или `Cmd+D` (Mac).[123]
4. На телефоне: в Chrome на Android нажмите «Ещё» (три точки справа от адресной строки) ⊠ «Добавить в закладки».[124] В Safari на iPhone нажмите «Поделиться» ⊠ «Добавить заклад-

[123] Справка Chrome: быстрые клавиши, «Добавить текущую веб-страницу в закладки»: Ctrl + D на Windows и Linux, ⊠ + D на Mac. Проверено: 2026-10-13.

[124] Добавить закладку в Chrome, Справка Google, на Android значок «Ещё» справа от адресной строки ⊠ «Добавить в закладки». Проверено: 2026-10-13.

ку».[125]

5. Дальше заходите в почту и в банк на компьютере только из закладки, каждый раз, без нового набора адреса и без ссылки из письма.

Результат: на телефоне вы входите в банк через его приложение, а сайты почты и банка лежат в закладках.

Если не получилось. Приложение банка не открывается — зайдите на сайт банка из закладки (шаги 2–4).

Получилось — когда банк открывается из приложения или закладки, почта лежит в закладках браузера или телефона, и заходить вы теперь будете оттуда, а не по ссылке из письма.

Проверить странное сообщение от знакомого

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, «неудобно сейчас звонить». Узнавать почерк того, кто пишет, здесь бесполезно — пишет не он, а тот, кто получил доступ к переписке.

Базовый минимум.

1. Деньги не переводите, пока человек не подтвердил просьбу голосом.
2. Не отвечайте в том же чате, а позвоните человеку на номер, который уже есть в контактах.
3. Трубку не берут, а деньги нужны «прямо сейчас» — не переводите. Настоящий знакомый перезвонит и подтвердит или опровергнет просьбу одним вопросом.

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

[125] Справка Apple: добавление веб-страниц в закладки в Safari на iPhone, на странице названы «Поделиться» и «Добавить закладку»; порядок нажатий в доступной части текста не приведён. Проверено: 2026-10-13.

— то же самое, что пароль, только одноразовое: его не называют никому и никогда, ни «поддержке», ни знакомому, каким бы срочным ни казался повод.[126] Тот же принцип держит и «Облачный пароль»[127] в Telegram из темы про двухфакторную аутентификацию: второй замок работает только до тех пор, пока его секрет знаете вы одни.

Позвонить по известному номеру

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).

Записать номер стоит прямо сейчас, пока карта под рукой, а не в момент, когда придёт то самое письмо и разбираться будет уже некогда.

Базовый минимум.

1. Переверните карту и найдите номер телефона банка на обратной стороне.
2. Добавьте его в контакты телефона и подпишите «Банк».
3. При сомнениях в письме или звонке звоните только по этому номеру и спросите оператора, писал ли вам банк. Настоящий банк подтвердит или опровергнет письмо за один вопрос.

Если не получилось. На карте нет номера — возьмите его из договора с банком; номер из письма и из поиска не используйте.

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

[126] Telegram FAQ, на англ. Проверено: 2026-10-12.
[127] Telegram FAQ (русская версия). Проверено: 2026-10-11.

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

Дополнительно (на выбор): номер с официального сайта банка. Берите, если карты под рукой нет: зайдите на сайт банка через закладку (не по ссылке из письма) и возьмите номер в его разделе контактов.

Максимум

Дополнительно: публичный Wi-Fi. 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.

Правило одно: на публичном Wi-Fi банк, почту и оплату не открывайте. Переключитесь на мобильный интернет на те пару минут, что нужны для входа, а к Wi-Fi вернитесь потом, для всего остального.

Если браузер всё же показал предупреждение о сертификате (страница сообщает, что подключение не защищено или сертификат не подтверждён), не нажимайте «всё равно продолжить» ни при каких условиях: закройте вкладку и зайдите в банк или почту из закладки на мобильном интернете. В этот момент браузер буквально не может подтвердить, с кем вы разговариваете. (⊠ атака посредника).

Страница-заглушка, которая просит войти в сеть, бывает безобидной (гостиничный Wi-Fi иногда просит просто адрес почты), но если заглушка просит именно пароль от настоящей

почты — это уже не авторизация в сети, а форма для сбора паролей, наряженная под неё. Закройте её и переключитесь на мобильный интернет.

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

Что делать после ввода пароля

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

Порядок. Ввели данные карты или деньги уже ушли — начните с шага 1 и сразу переходите к остальным. Ввели только пароль — начните с шага 2. Шаги идут по порядку.

Шаг 1. Банк (только если затронута карта или ушли деньги). Немедленно позвоните по номеру из контактов («Банк»), который вы записали 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, 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 нужно сразу, не откладывая на «сначала успокоюсь».

Шаг 2. 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. Буфер обмена KeePassXC очистит сам через 10 секунд после копирования (значение по умолчанию).[128] Результат: вход успешен, а существующая запись содержит актуальный пароль.

Если не получилось. Сайт не принимает новый пароль — запись в базе не меняйте и повторите смену с пункта 1 этого списка.

Шаг 3. Тот же пароль на других сайтах. Если этот пароль вы использовали ещё где-то, смените его и там по тому же списку, начав с почты — через неё сбрасывают пароли всех остальных сервисов. Как перестать повторять пароли — в теме про пароли.

Шаг 4. Выгнать того, кто мог войти по старому паролю раньше, чем вы его сменили: смена пароля новый вход не пускает, а уже открытые чужие сессии Google после неё завершает в основном, но не все (подтверждённые устройства остаются)[129], поэтому список устройств проверьте вручную.

Gmail: выйти со всех чужих сеансов и проверить следы взлома

1. Откройте аккаунт Google ⊠ «Безопасность и вход в аккаунт» ⊠ блок «Ваши устройства» ⊠ «Управление всеми устройствами»: видно каждое устройство с открытым входом, и на любом из них, кроме своего, можно нажать «Выйти».[130]

[128] KeePassXC, исходный код настроек (Config.cpp): очистка буфера обмена включена по умолчанию, срок ClearClipboardTimeout равен 10 секундам, на англ. Проверено: 2026-10-13.

[129] Что делать при смене пароля аккаунта Google, Справка Google. Проверено: 2026-10-11.

[130] Устройства с доступом к аккаунту Google, Справка Google, «Безопасность и вход в аккаунт» ⊠ «Ваши устройства» ⊠ «Управление всеми устройствами» ⊠ «Вый-

2. Внизу главной страницы Gmail есть строка о последней активности аккаунта со ссылкой «Подробные сведения» — откройте её: там видно, если аккаунт открыт ещё где-то.[131]
3. Шестерёнка вверху справа ⊠ «Все настройки» ⊠ вкладка «Пересылка и POP/IMAP»: проверьте, не появился ли там чужой адрес для пересылки писем. Нашли чужой — удалите.[132] Чужую пересылку добавляют, чтобы читать вашу почту и после смены пароля. *(вывод автора)*
4. Там же — вкладка «Фильтры и заблокированные адреса»: удалите все фильтры, которых не заводили сами.[133] Фильтр может молча архивировать или удалять письма от банка, чтобы вы не заметили предупреждений. *(вывод автора)*
5. В «Безопасности и входе в аккаунт» откройте блок «Вход в Google» ⊠ «Резервный номер телефона» и «Резервный адрес электронной почты»: если там чужой номер или адрес, нажмите значок «Удалить» (или «Изменить» — карандаш) и впишите свой. Если их подменили, вернуть аккаунт станет сложнее даже тогда, когда пароль уже снова ваш.[134]

Официально: устройства в аккаунте Google, пересылка писем, фильтры, резервный телефон и почта.

То же самое для Telegram: откройте «Настройки» ⊠ «Устройства» (Devices) и завершите каждый сеанс, который вы не узнаёте, оставив только свой телефон.[135]

Если не получилось. Пункта «Устройства» нет — откройте «Конфиденциальность» ⊠ «Активные сеансы» (Privacy & Security > Active

---

ти». Проверено: 2026-10-13.

[131] Последние действия в аккаунте Gmail, Справка Google. Проверено: 2026-10-12.

[132] Автоматическая пересылка писем в Gmail, Справка Google. Проверено: 2026-10-11.

[133] Фильтры в Gmail, Справка Google. Проверено: 2026-10-11.

[134] Справка Google: резервный телефон и резервная почта, «Безопасность и вход в аккаунт» ⊠ «Вход в Google» ⊠ «Резервный номер телефона» и «Резервный адрес электронной почты», значки «Изменить» и «Удалить». Проверено: 2026-10-13.

[135] Telegram FAQ, путь «Settings > Devices», сеанс на отдельном устройстве можно завершить; подпись кнопки завершения всех других сеансов на странице не приведена, на англ. Проверено: 2026-10-13.

Sessions).[136]

> **Максимум**
>
> **Дополнительно: почта не Gmail.** Для другого почтового сервиса чужие входы, пересылку и фильтры проверяют по тому же плану, что в блоке про Gmail: список устройств или сеансов, адрес пересылки, правила и фильтры, телефон и почта для восстановления. Названия пунктов у каждого сервиса свои и в этой теме не разобраны: ищите разделы «Безопасность» и «Настройки почты». *(вывод автора)*

> **Максимум**
>
> **Дополнительно: сообщить о фишинговой странице.** Саму поддельную страницу 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.

Шаги 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 приложение банка или 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.

[136]Telegram FAQ, альтернативный путь «Privacy & Security > Active Sessions», на англ. Проверено: 2026-10-13.

Резервные копии

Телефон можно уронить в раковину, оставить в такси или разбить — и десять лет фотографий пропадут 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

Сделать три копии на двух носителях

Правило трёх копий звучит как считалка, но в ней ровно три числа, и все три важны: минимум три экземпляра данных, включая рабочий; минимум два разных типа носителей; минимум один экземпляр вне дома.[137] (☒ правило 3-2-1).

Базовый минимум. Ваша схема — одна, без вариантов:

[137] CISA, Data Backup Options (PDF), правило 3-2-1: три копии, два типа носителей, одна копия вне дома или офиса, на англ. Проверено: 2026-10-13.

1. Копия 1 — рабочая: файлы и фотографии там, где вы ими пользуетесь каждый день (телефон и компьютер).
2. Копия 2 — облако, то есть вне дома: iCloud на iPhone, Google на Android. Включается в разделах про телефон и про фотографии ниже.
3. Копия 3 — внешний жёсткий диск, который лежит отключённым в ящике стола. Настраивается в разделе про диск ниже.

Результат: у файлов и фотографий телефона есть все три места. У файлов компьютера — два: рабочее и диск; третьим может стать облачная копия базы паролей (блок «Дополнительно» в разделе про базу паролей). Всё остальное в теме — про то, как включить каждое из мест по отдельности.

Видео: Обучение системных администраторов — Как не потерять данные: резервное копирование и правило 3-2-1 простыми словами https://www.youtube.com/watch?v=GqCoVdm6odE

Обучение системных администраторов — Как не потерять данные: резервное копирование и правило 3-2-1 простыми словами — подсказка к правилу трёх копий и к проверке копии; остальное в ролике (серверы, программы для администраторов) к вашей схеме не относится.

- 7:14 — правило 3-2-1
- 9:40 — копия, которую ни разу не восстанавливали, копией не считается

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.

> **Максимум**

Дополнительно: почему диск должен быть отключён. Для защиты от шифровальщика к правилу трёх копий добавляют ещё хотя бы одну офлайн-копию: носитель отключён и недоступен для случайного удаления или шифровальщика.[a] В вашей схеме это диск из копии 3. Вне дома и офлайн могут быть разные копии: облако — вне дома, диск в ящике — офлайн.

[a] CISA, #StopRansomware Guide, офлайн-копии как защита от шифровальщика; сама формула 3-2-1 там не разбирается, на англ. Проверено: 2026-10-13.

Проверить резервную копию телефона

На современном телефоне копия самого устройства (настройки, контакты, данные приложений) и синхронизация фотографий — два разных переключателя. Здесь включается первый; фотографии — в разделе про фото ниже. Если «Фото iCloud» на iPhone включено, фото и видео в копию устройства не входят: они хранятся отдельно.[138]

Базовый минимум.

iPhone: резервная копия в iCloud

1. Подключите iPhone к Wi-Fi.
2. «Настройки» ☒ ваше имя вверху ☒ iCloud ☒ «Резервная копия в iCloud». Включите переключатель «Резервное копирование этого iPhone».[139] (☒ резервная копия в iCloud).
3. Нажмите «Создать резервную копию» и дождитесь окончания. Дата и время последней копии показаны в том же разделе.
4. Дальше копия делается сама, когда iPhone стоит на зарядке, подключён к Wi-Fi и заблокирован: оставляйте его так на

[138] Справка Apple: резервное копирование iPhone в iCloud, без «Фото iCloud» снимки сохраняются в копии устройства. Проверено: 2026-10-13.

[139] Справка Apple: как включить резервное копирование в iCloud, путь «Настройки» ☒ имя ☒ iCloud и условия автоматической копии (питание, Wi-Fi, заблокированный экран); на странице экран назван и «Резервная копия в iCloud» (в шагах ручной копии), и «Резервное копирование iCloud» (в автоматической); в тексте взято первое. Проверено: 2026-10-13.

ночь.

Если места в iCloud не хватает, iPhone покажет предупреждение — докупите минимальный тариф по правилу из раздела про фото ниже.

Официально: как включить резервное копирование в iCloud.

Видео: AppleTheme — Способы резервного копирования перед обновлением на iOS 18! Как создать резервную копию iOS https://www.youtube.com/watch?v=LVUl0M25v6s

AppleTheme — Способы резервного копирования перед обновлением на iOS 18! Как создать резервную копию iOS — подсказка к включению копии iPhone в iCloud; остальные способы из ролика (Finder, iTunes, сторонние программы) здесь не нужны.

- 0:36 — Настройки ⊠ учётная запись ⊠ iCloud ⊠ Резервная копия в iCloud

Android: резервная копия в аккаунт Google

1. «Настройки» ⊠ Google ⊠ «Все сервисы» ⊠ «Резервное копирование». Включите резервное копирование Google One.[140] (⊠ настройки Google).
2. Нажмите кнопку немедленной копии («Back up now» в английской справке) — один раз, чтобы не ждать ночи. (⊠ начать копирование).
3. На том же экране проверьте, что в копию входят приложения и их данные, журнал вызовов, контакты, настройки и SMS/MMS. Фото и видео сюда не входят: они копируются отдельным переключателем в Google Фото (раздел про фото ниже).
4. Бесплатных гигабайт у Google пятнадцать, и они общие на почту, Диск и Фото разом: это потолок, о котором говорит раздел про фото.

Если не нашли пункт «Резервное копирование» — введите «резервное копирование» в поиске по настройкам. Samsung Cloud вместо

[140] Справка Android: резервное копирование данных, путь Settings ⊠ Google ⊠ All services ⊠ Backup, кнопка Back up now, состав копии; русские подписи страница не приводит, на англ. Проверено: 2026-10-13.

аккаунта Google — в блоке «Дополнительно» ниже.

Официально: резервное копирование данных Android — страница на английском.

Видео: HardReset_info Ukraine — Как включить синхронизацию резервных копий гугл на Android 13 / Резервное копирование гугл Android13 https://www.youtube.com/watch?v=QfkIHZSyPTM

HardReset_info Ukraine — Как включить синхронизацию резервных копий гугл на Android 13 / Резервное копирование гугл Android13 — подсказка к копии Android в аккаунт Google; показан Android 13, подписи пунктов у вашей версии могут отличаться.

- 0:14 — Настройки ☒ Google
- 0:21 — Резервное копирование ☒ Начать копирование

Переписка в мессенджерах в общую копию телефона не попадает: у каждого мессенджера своя копия. Итог одной строкой: в Telegram делать ничего не нужно; в WhatsApp — включить копию с шифрованием; Signal — только если вам нужна его копия, это в блоке «Дополнительно» ниже.

Telegram: делать ничего не нужно

1. Ничего не включайте: обычные чаты Telegram живут в его облаке и появятся сами на любом новом устройстве, стоит туда войти.[141]
2. Секретные чаты существуют только на том телефоне, где заведены, исчезают вместе с ним и стираются при выходе из аккаунта.[142] Переписку, которую нельзя потерять, ведите в обычном чате, а не в секретном. *(вывод автора)*

Экспорт переписки с компьютера — в блоке «Дополнительно» ниже.

WhatsApp: включить копию и зашифровать её

[141] Telegram FAQ, обычные чаты хранятся в облаке, на англ. Проверено: 2026-10-13.

[142] Telegram FAQ, секретные чаты только на устройстве создания, при выходе теряются, на англ. Проверено: 2026-10-13.

1. Откройте «Настройки» ⊠ «Чаты» ⊠ «Резервная копия» и включите копирование: на Android — в Google Диск, на iPhone — в iCloud. Выберите ежедневную периодичность (в английской версии — Daily).[143] Копия займёт место в тех же бесплатных гигабайтах, что и остальное. (⊠ раздел «Резервная копия чатов»).
2. В том же разделе включите «Резервное копирование со сквозным шифрованием» ⊠ «Включить». Без этого шага копия технически доступна Google или Apple, а не только вам. (⊠ шифрование копии).
3. Выберите защиту паролем. Сначала сгенерируйте пароль в KeePassXC из темы про пароли и сохраните его в базу, затем введите его в WhatsApp. Забудете пароль — копию не откроет никто, включая сам WhatsApp.[144] (⊠ пароль копии).

Официально: про сквозное шифрование резервных копий.

Видео: Всё про Андроид — Как зашифровать резервные копии WhatsApp на Google Диске https://www.youtube.com/watch?v=PXN1j1FMMH8

Всё про Андроид — Как зашифровать резервные копии WhatsApp на Google Диске — подсказка к шифрованию копии WhatsApp на Android (копия в Google Диск); на iPhone порядок тот же, но копия хранится в iCloud.

- 0:45 — Чаты ⊠ Резервная копия чатов
- 1:27 — копирование с шифрованием ⊠ Включить
- 1:50 — пароль для копии

Получилось — когда в настройках телефона напротив резервной копии устройства значится «Включено», у неё есть дата последней

[143] Справка WhatsApp: резервная копия, защищённая сквозным шифрованием, путь «Настройки» ⊠ «Чаты» ⊠ «Резервная копия»; периодичность daily, weekly или monthly названа на странице «How to back up your chat history», страницы WhatsApp не открылись, поэтому русские подписи пути, периодичности и пункта «Резервное копирование со сквозным шифрованием» не подтверждены, на англ. Проверено: 2026-10-13.

[144] WhatsApp, End-to-end encrypted backups, шифрование включается вручную, без пароля или ключа копию не прочитает ни WhatsApp, ни хранилище, на англ. Проверено: 2026-10-13.

копии, а в WhatsApp включено шифрование копии. Это разные «включено», и одного из них мало.

Максимум

Дополнительно (на выбор): Samsung Cloud вместо аккаунта Google. Берите, если вы пользуетесь Samsung и хотите копию настроек у Samsung. «Настройки» ⊠ имя вашей учётной записи Samsung вверху ⊠ Samsung Cloud ⊠ «Back up data» ⊠ отметьте данные ⊠ «Back up now». Автокопия идёт раз в сутки при трёх условиях разом: телефон на Wi-Fi, стоит на зарядке и с выключенным экраном, то есть ночью.[a] Подписи на странице Samsung английские, русские не подтверждены; переключатель автокопии на ней называется «Auto back up while roaming».

[a] Samsung: резервное копирование данных, раз в сутки, Wi-Fi, зарядка, экран выключен; переключатель автокопии на странице называется «Auto back up while roaming», хотя описан как ночная копия по Wi-Fi, на англ. Проверено: 2026-10-13.

Максимум

Дополнительно (на выбор): Signal. Берите, если важна история переписки в Signal. Secure Backups анонсированы 8 сентября 2025 года (тогда — бета на Android): бесплатно хранятся все тексты (до 100 МиБ) и медиа за последние 45 дней, платно (1,99 $ в месяц) — больше, до 100 гигабайт.[a] Включение: в Signal «Settings» ⊠ «Backups» ⊠ «Setup» ⊠ «Enable Backups» ⊠ сохранить ключ восстановления.[b] Ключ — 64 символа, создаётся на самом устройстве, и потерянный ключ не восстановит даже сама Signal; сохраните его в базу паролей. Эта часть Signal меняется от версии к версии чаще остального. *(вывод автора)*

[a] Signal, Introducing Signal Secure Backups, пост от 8 сентября 2025: бесплатно все тексты (до 100 МиБ) и медиа за последние 45 дней, 1,99 $ в месяц, до 100 ГБ платно; на тот момент опробовать могли только пользователи беты Signal на Android, на англ. Проверено: 2026-10-13.

[b]Справка Signal: Secure Backups, путь Settings ⊠ Backups ⊠ Setup ⊠ Enable Backups, все тексты и медиа за последние 45 дней бесплатно, на англ. Проверено: 2026-10-13.

Максимум

Дополнительно (на выбор): экспорт Telegram. Берите, если хотите хранить переписку у себя. Telegram Desktop ⊠ «Настройки» ⊠ «Экспорт данных Telegram»; формат выберите HTML: он читается без программ. На выходе папка с перепиской и вложениями, которую кладут на внешний диск вместе с остальным.[a] Официально: про экспорт данных — страница на английском, 2018 года.

[a]Telegram, Export and more, статья 2018 года: путь «Settings ⊠ Export Telegram data», форматы JSON и HTML; в новых версиях путь может отличаться, на англ. Проверено: 2026-10-13.

Максимум

Дополнительно (на выбор): WhatsApp другой периодичности, ключ вместо пароля. Периодичность «Еженедельно» или «Ежемесячно» берите, если чаты почти не меняются. Вместо пароля можно выбрать 64-значный ключ: берите, если не хотите хранить пароль в базе, но ключ придётся хранить так же надёжно.

Максимум

Дополнительно: когда менять телефон. Если производитель больше не выпускает обновления безопасности или до конца срока осталось меньше года, сделайте копию по шагам выше и подберите замену. Страницы сроков — в теме про обновления. *(вывод автора)*

Настроить копирование на внешний диск

Копия 3 — 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 там, где облачная бессильна.

Базовый минимум.

1. Узнайте объём встроенного накопителя компьютера (полный, а не занятый). Mac: «Системные настройки» ⊠ «Основные» ⊠ «Хранилище». Windows: «Параметры» ⊠ «Система» ⊠ «Хранилище».
2. Купите портативный жёсткий диск (HDD, подключение по USB) вдвое больше этого объёма, округлив вверх до 2 или 4 терабайт: Apple требует для Time Machine накопитель минимум вдвое больше хранилища Mac.[145] Запас уходит на копии разных дат и на рост данных. Например, портативные HDD Toshiba Canvio, Seagate Expansion Portable, WD My Passport и Elements; наличие в вашем магазине проверьте. Флешку и внешний SSD под эту копию не берите: они хранят данные зарядом, который без питания со временем утекает, а диск лежит в ящике месяцами. *(вывод автора)*
3. Поставьте в календаре телефона повторяющееся напоминание «Подключить диск» на воскресенье, раз в неделю. *(вывод автора)*
4. Настройте автокопирование по инструкции для вашей системы ниже.
5. После первой копии извлеките диск и уберите его в ящик: пока он подключён, заражённый компьютер может зашифровать и его, а отключённый диск шифровальщик не достанет.[146]

Mac: Time Machine

1. Подключите новый или пустой диск. Mac может предложить

[145] Справка Apple: резервное копирование Mac с помощью Time Machine, накопитель минимум вдвое больше хранилища Mac. Проверено: 2026-10-13.

[146] CISA, #StopRansomware Guide, шифровальщики добираются до доступных копий; офлайн-копия защищена, пока отключена, на англ. Проверено: 2026-10-13.

стереть его: это удаляет все файлы на диске, поэтому если там есть нужное — сначала скопируйте это в другое место. (☒ форматирование диска).

2. Меню Apple ☒ «Системные настройки» ☒ «Основные» ☒ «Time Machine». Нажмите кнопку «+», выберите диск и «Настроить диск».[147] (☒ выбор диска).
3. В окне настройки включите шифрование резервных копий и задайте пароль. Сразу сохраните пароль в базу KeePassXC: он понадобится при каждом подключении диска к Mac, а потерянный пароль означает потерянную копию.[148] (☒ шифрование копий).
4. Расписание настраивать не нужно: 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.[149]
5. Чтобы запустить копию сразу, выберите в меню Time Machine в строке меню «Создать резервную копию сейчас». (☒ значок в строке меню).

Если значка Time Machine нет в строке меню, включите его: «Системные настройки» ☒ «Пункт управления».

Официально: как настроить Time Machine.

Видео: 7 Тем — Резервное копирование данных Macbook, iMac, Mac mini (Time Machine) https://www.youtube.com/watch?v=bZCBqq013pM

7 Тем — Резервное копирование данных Macbook, iMac, Mac mini (Time Machine) — подсказка к Time Machine; в ролике более старый вид «Системных настроек», подписи пунктов могут отличаться.

- 0:38 — Time Machine ☒ выбор диска

[147] Справка Apple: резервное копирование Mac с помощью Time Machine, путь «Системные настройки» ☒ «Основные» ☒ «Time Machine», кнопка «+», «Настроить диск». Проверено: 2026-10-13.

[148] Справка Apple: выбор диска для резервной копии и параметры шифрования, пароль нужен при подключении диска; точная подпись флажка шифрования на странице не приводится, на англ. Проверено: 2026-10-13.

[149] Справка Apple: резервное копирование Mac с помощью Time Machine, хранение копий по часам, дням и неделям. Проверено: 2026-10-13.

- 1:07 — диск придётся стереть
- 1:43 — шифрование копий
- 3:15 — значок в строке меню и ручная копия
- 3:42 — просмотр и восстановление файлов

Windows: «История файлов» на внешний диск

1. Установите все обновления Windows: после обновления за сентябрь 2026 года «История файлов» у части пользователей переставала создавать копии, и проблема исправлена в обновлениях с 22 сентября 2026 года.[150]
2. Подключите диск. (☒ отдельный диск для истории файлов).
3. «Панель управления» (найдите по названию через поиск в меню «Пуск») ☒ «Система и безопасность» ☒ «Сохранить резервные копии файлов с помощью журнала файлов». Если диск не выбран автоматически, нажмите «Выбрать диск» и укажите его. Нажмите «Включить».[151] (☒ включение истории файлов).
4. Копируются основные папки: «Документы», «Рисунки», «Видео», «Музыка»; справка называет среди них и «Рабочий стол». (☒ какие папки копируются). Всё важное держите в «Документах». Частоту копий и срок хранения версий не меняйте. *(вывод автора)*
5. После «Включить» копирование идёт само, пока диск подключён. *(вывод автора)*

Если дата последней копии не обновляется, а Windows просит подключить диск заново, установите последние обновления Windows и подключите диск снова.

Официально: резервное копирование и восстановление с помощью истории файлов.

[150] Microsoft: история обновлений Windows 11 версии 26H2, «История файлов может перестать работать после установки обновления за сентябрь 2026 г.». Проверено: 2026-10-13.

[151] Microsoft: резервное копирование и восстановление с помощью истории файлов, «Система и безопасность», «Выбрать диск», «Включить»; «Рабочий стол» назван среди основных папок в разделе «Настройка журнала файлов»; пункта «Запустить сейчас» на странице нет; значения частоты и срока хранения по умолчанию страница не называет. Проверено: 2026-10-13.

Видео: remontka.pro video — История файлов Windows 11 и Windows 10 — встроенная функция резервного копирования и восстановления https://www.youtube.com/watch?v=xDFQEx9gylc

remontka.pro video — История файлов Windows 11 и Windows 10 — встроенная функция резервного копирования и восстановления — подсказка к «Истории файлов»; в ролике копии пишутся на флешку, вам нужен внешний жёсткий диск.

- 0:39 — какие папки попадают в историю файлов
- 1:12 — Панель управления ⊠ История файлов
- 1:26 — отдельный физический диск
- 3:27 — восстановить прежнюю версию файла

Проверка (сразу после первой копии). Откройте диск с копией и достаньте из него одну случайную фотографию или документ. Mac: значок Time Machine в строке меню ⊠ просмотр резервных копий, найдите в «Документах» любой файл за сегодняшнюю дату. (⊠ просмотр копий Time Machine). Windows: в Проводнике щёлкните правой кнопкой по папке «Документы» ⊠ «Восстановить предыдущие версии» ⊠ вкладка «Предыдущие версии» ⊠ выберите версию и «Открыть в журнале файлов». (⊠ прежняя версия файла). Результат: файл есть в копии и открывается так же, как исходный. Один файл не доказывает, что скопировалось всё, но для первой проверки этого достаточно. Копия, которую ни разу не проверяли, — это не гарантия, а надежда, что в нужный момент она сработает. (⊠ копия, которую ни разу не восстанавливали). Повторяйте проверку раз в три месяца и поставьте на это второе повторяющееся напоминание в календаре. *(вывод автора)*

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

Отдельной системы под документы заводить не нужно — и когда тема про фишинг отправляет сюда за копией документов, она отправляет ровно к этому же диску. Сканы паспорта, договоры и рабочие файлы, которые лежат в «Документах», уезжают на диск тем же движением, что и всё остальное.

Получилось — когда диск настроен, первая копия сделана, один файл из неё открыт, а напоминание на воскресенье стоит в кален-

даре.

Максимум

Дополнительно (на выбор): шифрование диска в Windows. Берите, если диск выезжает из дома: лежит в рюкзаке, ездит на дачу, остаётся в машине. Потерянный диск без шифрования читается на любом чужом компьютере как обычная флешка, а с шифрованием — как кусок железа без вашего пароля. Если диск никогда не покидает дом, в Windows его можно не шифровать. В Windows нужен режим для съёмных дисков — BitLocker To Go, — а BitLocker в Windows доступен только в редакциях Pro, Enterprise и Education, в домашней его нет.[a] Поэтому в Windows Home зашифровать диск этим способом не получится; как поступить, если диск уже зашифрован на другом компьютере, проверьте до покупки. *(вывод автора)* Для Mac шифрование уже включено в базовых шагах выше. Зашифрованный диск при каждом подключении спрашивает пароль.

[a] Поддержка Microsoft, BitLocker Drive Encryption, «only available on devices running Windows Pro, Enterprise, or Education editions», в Home недоступен; съёмные диски — раздел «Removable data drives - BitLocker To Go»; BitLocker FAQ: BitLocker To Go — это BitLocker на съёмных дисках; работу такого диска в Home страницы не описывают, на англ. Проверено: 2026-10-13.

Максимум

Дополнительно: два соседа «Истории файлов» в Windows. Не путайте их с ней. «Резервное копирование Windows» («Пуск» ☒ «Параметры» ☒ «Учётные записи» ☒ «Резервное копирование Windows») копирует примерно те же папки не на ваш диск, а в OneDrive, где бесплатно пять гигабайт, и требует учётной записи Microsoft — официальное описание. «Архивация и восстановление (Windows 7)» в «Системе и безопасности» делает полный образ системы; это старый инструмент, оставленный для совместимости с Windows 7.

Максимум

Дополнительно: NAS. Берите, если у вас много данных на нескольких компьютерах и вы готовы повозиться. Домашний сетевой накопитель (NAS): два диска в зеркале (RAID 1) и программа для личного облака (у Synology это Synology Drive), а второе такое устройство стоит в другом месте и получает копии с сохранением прежних версий (у Synology — Hyper Backup или Snapshot Replication). Но RAID — не копия: он защищает от поломки диска, а не от случайного удаления, шифровальщика или пожара. Простая «синхронизация» двух устройств повторит и удаление, и шифрование, поэтому нужны хранимые версии или защищённые от удаления снимки. Перед покупкой проверьте список совместимых дисков.

Скопировать базу паролей в резерв

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.

Базовый минимум.

1. В KeePassXC сохраните изменения, заблокируйте базу и закройте программу.
2. Подключите внешний диск из предыдущего раздела и скопируйте на него файл `.kdbx` в отдельную папку. Файл уже зашифрован целиком, так что экспорт в CSV/XML для копии не нужен.[152] Если вы по теме про пароли держите копию и на флешке, это удобная дополнительная копия, но основной для долгого хранения служит диск: флешки хуже хранят данные без питания. *(вывод автора)*
3. Мастер-пароль на диск не записывайте: он остаётся в вашей памяти, а страховочный листок, если вы его завели по теме про пароли, лежит отдельно от диска.

[152] KeePassXC User Guide, на англ. Проверено: 2026-10-13.

4. Повторяйте копирование каждый раз, когда подключаете диск по воскресеньям, и сразу после того, как перенесли в базу новые пароли. *(вывод автора)*
5. Проверка: скопируйте файл с диска на рабочий стол, откройте его в KeePassXC с мастер-паролем и убедитесь, что видны не меньше трёх записей. Рабочую базу копией не заменяйте. Проверенную копию с рабочего стола удалите.
6. Результат: есть рабочая база и отдельная копия `.kdbx` на диске, которая открывается.

Копия не открывается при верном пароле — скопируйте файл заново при закрытом KeePassXC и повторите проверку. *(вывод автора)*

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

> **Максимум**
>
> **Дополнительно (на выбор): ключевой файл.** Берите, только если вы включали его в теме про пароли. Скопируйте key file на другую флешку, не на диск с `.kdbx`, и проверьте открытие с мастер-паролем и key file. Потеря key file означает потерю доступа, даже если мастер-пароль известен.

> **Максимум**
>
> **Дополнительно (на выбор): копия в облако.** Берите, если хотите копию вне дома сверх диска. Положите копию `.kdbx` в то облако, которым вы уже пользуетесь (iCloud или Google Диск): файл зашифрован, облако видит только его. Проверка та же: откройте облачную копию с мастер-паролем.

> **Максимум**
>
> **Дополнительно: проверка на втором устройстве.** Откройте

> копию `.kdbx` в KeePassXC на втором компьютере или в приложении на телефоне. Если второго устройства нет, достаточно проверки из базового шага 5.

Сохранить фото и важные файлы

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 можно, просто через отдельный поход в нужную организацию и потерянное время.

Универсального «значка облака» у снимка нет: в двух главных галереях проверка устроена по-разному, и в одной из них значок означает не то, что подсказывает интуиция.

Базовый минимум.

Google Фото: включить копирование, исходное качество, проверка

1. Откройте приложение «Google Фото» — не «Настройки» телефона: этот переключатель живёт только здесь. Нажмите значок профиля вверху ☒ «Настройки Google Фото» ☒ «Копирование в облако». Включите его.[153]
2. Там же откройте «Качество облачных копий» и выберите «Исходное качество»: снимки сохранятся в том разрешении, в котором сняты. Оно занимает место в хранилище аккаунта.[154]
3. Вернитесь на главный экран. Вверху показан статус: «Копирование в облако» — идёт, «Копирование завершено» — всё скопировано.
4. Найдите любой снимок годовой давности. В правом нижнем углу миниатюры стоит значок «Скопировано в облако»: логи-

[153] Справка Google Фото: как проверить резервное копирование, «Настройки Google Фото» ☒ «Копирование в облако», значок «Скопировано в облако», статусы копирования. Проверено: 2026-10-13.

[154] Справка Google Фото: как выбрать качество облачных копий, «Качество облачных копий», варианты «Исходное качество» и «Сжатие файлов». Проверено: 2026-10-13.

ка обратная привычной — значок означает «копия есть». Нет значка — копии этого снимка в облаке нет; вернитесь к шагу 1 и проверьте, что переключатель включён.

Официально: как проверить резервное копирование.

iPhone: Фото iCloud и статус всей медиатеки

1. «Настройки» ⊠ ваше имя вверху ⊠ iCloud ⊠ «Фото». Включите переключатель синхронизации этого iPhone.[155]
2. Откройте «Фото», вкладку «Коллекции», и нажмите кнопку профиля: статус медиатеки показан под именем — синхронизировано всё или загрузка ещё идёт.[156] На iOS 17 и старше то же лежит в другом месте: вкладка «Медиатека», раздел «Все фото», прокрутить в самый низ.
3. Статус в iPhone показан для всей медиатеки, а не у каждого снимка.

Официально: синхронизация фото с iCloud.

Если ваши данные только в Google. Облако не заменяет копию. Данные выбранных сервисов аккаунта Google можно выгрузить через Google Takeout на свой диск, а не в тот же Google Диск: так у вас остаётся копия, не зависящая от Google. Если данных много, архив делится на части.[157]

Если места не хватает. Бесплатного места у большинства сервисов немного: у iCloud это пять гигабайт,[158] у Google пятнадцать, и те общие на почту, Диск и Фото,[159] а десять лет фотографий туда не влезают. Когда место кончается, копирование останавливается, а вместо рабочей копии остаётся уведомление о нехватке места, которое легко не замечать месяцами. *(вывод автора)* Правило одно:

[155]Справка Apple: настройка Фото iCloud на всех устройствах, «Настройки» ⊠ имя ⊠ iCloud ⊠ «Фото». Проверено: 2026-10-13.

[156]Справка Apple: «Фото iCloud», статус синхронизации в «Коллекциях» под именем профиля, на iOS 17 и старше во вкладке «Медиатека». Проверено: 2026-10-13.

[157]Справка Google: экспорт данных аккаунта, при большом объёме создаётся несколько архивов. Проверено: 2026-10-13.

[158]Apple, iCloud, бесплатный тариф 5 ГБ, на англ. Проверено: 2026-10-13.

[159]Справка Gmail: как устроено хранилище Google, до 15 ГБ на аккаунт, общие для Диска, Gmail и Google Фото. Проверено: 2026-10-13.

не выключайте копирование и не переходите на сжатие, а докупите минимальный тариф, которого хватает вашим фотографиям. Платные тарифы есть у обоих сервисов, актуальные цены смотрите на страницах тарифов: Google One и iCloud+.

Получилось — когда вы точно знаете: пропади телефон прямо сейчас, фотографии всё равно останутся в облаке. Пока этого нет, настройка не закончена.

Максимум

Дополнительно (на выбор): «Сжатие файлов» вместо исходного качества. Берите, если докупать место не хотите: фото больше 16 Мпкс уменьшатся до этого размера, видео выше 1080p — до 1080p, но такие файлы тоже занимают место в хранилище.[a] Для печати большого формата и для снимков выше 16 Мпкс оставляйте «Исходное качество».

[a] Справка Google Фото: как выбрать качество облачных копий, «Сжатие файлов» уменьшает фото до 16 Мпкс и видео до 1080p, но тоже занимает место. Проверено: 2026-10-13.

Максимум

Дополнительно (на выбор): повторяющаяся выгрузка Google Takeout. Берите, если не хотите каждый раз вспоминать про выгрузку сами: в настройках экспорта выберите повторяющийся экспорт вместо разового, и Google создаст архив выбранных данных каждые 2 месяца в течение года, первый архив сразу. Повторяющийся экспорт недоступен, если на аккаунте включена программа дополнительной защиты (Advanced Protection).[a] Через год создайте экспорт заново. *(вывод автора)*

[a] Справка Google: экспорт данных аккаунта, повторяющийся экспорт «every 2 months for one year», первый архив создаётся сразу; недоступен при включённой программе Advanced Protection, на англ. Проверено: 2026-10-25.

Максимум

Дополнительно: проверка облачной копии телефона. Файл из копии устройства отдельно, как правило, достать нельзя: она хранится единым образом и восстанавливается на телефон целиком, при настройке нового. *(вывод автора)* Ближайшая честная замена — открыть облачную галерею (icloud.com или Google Фото) с чужого устройства и увидеть там свои снимки. Это проверка того, что фотографии успевают синхронизироваться, а не самой копии устройства.

Максимум

Дополнительно: что будет с копиями, если с вами что-то случится. Тема неприятная и потому откладывается навсегда: близким понадобится доступ к фотографиям и документам. Решается парой строк на бумаге в закрытом ящике дома: где лежит копия и как до неё добраться. Написать один раз и больше не возвращаться к этой мысли — задача именно такая.

Зачем нужны копии

Шифровальщик — вредоносная программа, которая шифрует файлы и требует денег за расшифровку. Раньше это была тема для служб безопасности крупных компаний — целились туда, где можно потребовать выкуп посерьёзнее. Это давно не так: шифровальщики атакуют организации любого размера, а ноутбук с фотографиями и рабочими документами тоже годится для шантажа.[160]

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 шифро-

[160]CISA, #StopRansomware Guide, шифровальщики затрагивают организации любого размера, на англ. Проверено: 2026-10-13.

вальщику добраться до файлов, зато лишает вымогателя главного рычага — отказа вернуть ваши файлы. *(вывод автора)* Стёрли, зашифровали, потребовали денег — а у вас всё это время лежит отдельная копия, до которой он не дотянулся. От публикации украденных данных копия не защищает.

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.

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 устроено большинство людей. 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 раз в неделю подключить диск. 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 по короткой записи. 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

Проверить звонок обратным звонком

Правило одно: просят деньги, код или срочную помощь — положите трубку и перезвоните сами. Голос в трубке не доказательство: в исследовательской модели VALL-E для подделки голоса хватило записи длиной 3 секунды.[161] Видеозвонок тоже не доказательство, картинку подделывают так же.

[161] Neural Codec Language Models are Zero-Shot Text to Speech Synthesizers (VALL-E), arXiv:2301.02111, в аннотации: «only a 3-second enrolled recording of an unseen speaker»; результат исследовательской модели, не готового сервиса, на англ. Проверено: 2026-10-13.

Это не теория. В начале 2024 года сотрудник гонконгского офиса британской инженерной компании Arup[162] подключился к видеоконференции, где «финансовый директор» и «коллеги» оказались дипфейками.[163] По их указаниям он сделал 15 переводов на сумму около 200 млн гонконгских долларов (около 25 млн долларов США); обман вскрылся, когда сотрудник обратился в головной офис.[164]

Базовый минимум.

1. Завершите звонок или видеозвонок. Разговор не продолжайте, деньги и коды не называйте.
2. Откройте приложение «Контакты» на телефоне, найдите человека по имени и нажмите «Позвонить». Номер берите только из контактов: не из истории вызовов и не из присланного сообщения.
3. Если человека или номера в контактах нет — деньги не переводите, пока не получите номер у того, кто знает этого человека лично.
4. Когда дозвонились, спросите: «Ты только что звонил и просил деньги?» Только после ответа «да» обсуждайте перевод.
5. Один раз скажите это правило вслух всем, кто живёт с вами, и напишите его в семейный чат одной строкой: «Деньги — только после звонка на номер из контактов».

Типовой сбой: человек не берёт трубку. Деньги не переводите, пока не дозвонились лично: спешка и давление — типичный приём таких схем. *(вывод автора)*

Получилось — когда все, кто живёт с вами, знают правило из шага 5 и оно записано в семейном чате.

[162]Пересказ в Fortune: Arup, жертва дипфейк-мошенничества и Пересказ в CFO Dive: материал Financial Times, оба на англ.; подтверждают, что жертвой стала Arup; вторичные источники, заявление Arup и пресс-релиз полиции для проверки не открылись. Проверено: 2026-10-12.

[163]Пересказ в The Register: Hong Kong deepfaked CFO, на англ. Пересказ сообщения полиции Гонконга (февраль 2024, компания в нём не названа); первоисточники (полиция Гонконга, Arup) для проверки не открылись. Проверено: 2026-10-12.

[164]Пересказ в Fortune: Arup, жертва дипфейк-мошенничества и Пересказ в The Register: Hong Kong deepfaked CFO, оба на англ.; число переводов, сумма и обращение в головной офис указаны в обоих; вторичные источники, первоисточники для проверки не открылись. Проверено: 2026-10-12.

Максимум

Дополнительно (на выбор): в контактах нет номера. Критерий выбора — кто просит. Человек из семьи или с работы: позвоните тому, кто знает его лично, и попросите назвать номер или передать, чтобы он позвонил вам сам. Банк или служба: позвоните по номеру с оборота карты или с официального сайта организации, а не по тому, что назвали в разговоре. *(вывод автора)*

Договориться о контрольном слове

Контрольное слово помогает быстро заподозрить подделку, но обратный звонок не заменяет: для денег он обязателен даже тогда, когда слово названо верно.

Базовый минимум.

1. Придумайте слово из двух-трёх случайных слов, не связанных с вами: не имя, не кличка питомца, не девичья фамилия, не дата. Пример формы: «фиолетовый бегемот». Этот пример уже опубликован, возьмите своё. *(вывод автора)*
2. Соберите всех, кого касается: тех, кто живёт с вами, и до пяти близких, кому вы звоните чаще всего. Скажите слово вслух при личной встрече; каждый повторяет его вслух. *(вывод автора)*
3. Слово не пишите в чат и не храните в заметках телефона: его знают только те, кто слышал его вслух. *(вывод автора)*
4. Договоритесь о порядке: если кто-то просит деньги или срочную помощь, вы просите его назвать слово. Слово называет звонящий сам, без подсказки.
5. Скажите вслух: «Спрашивать слово — не обидно». Слово не названо или названо неверно — положите трубку и перезвоните по номеру из контактов (раздел выше).

Типовой сбой: близкий забыл слово. Это не повод переводить деньги: перезвоните по номеру из контактов и обсуждайте дальше только после этого.

Получилось — когда слово придумано и каждый, кого оно касается, один раз повторил его вслух.

Максимум

Дополнительно (на выбор): вопросы вместо слова. Берите, если близкий не запомнит слово, например пожилой родственник. Заранее договоритесь о двух-трёх вопросах про то, чего на самом деле нет: «как там Вулфи?» (собаки давно нет), «не забыл полить цветы у бабушки?», «как прошёл футбол во вторник?» (никакого футбола не было). Задавайте один вскользь, голосом обычной заботы. Свой человек растеряется и поправит: «Какой Вулфи?»; подделка с большей вероятностью поддержит тему, о которой не знает. *(вывод автора)* Если вопрос уже «засветился», возьмите другой. Вопросы не публикуйте в соцсетях и не проговаривайте в голосовых.

Максимум

Дополнительно (на выбор): смена слова. Берите, если слово кто-то мог услышать со стороны или записать. Придумайте новое и повторите шаги 1–2. Без такого повода меняйте слово раз в год. *(вывод автора)*

Убрать лишнее из запроса чат-боту

Правило: не отправляйте в чат-бот ничего из этого списка: пароли и коды, паспортные данные, медицинские выписки, финансовые документы, рабочие документы, чужие переписки. Всё, что вы отправили в чат-бот, вы отправили в чужую компанию, а дальше это живёт по её правилам. Ваш разговор может уйти в обучение модели или к сотрудникам при проверке безопасности; а если закон требует, чаты могут храниться и дольше обычного.[165] Гарантий, что

[165] Claude: как долго хранятся мои данные («we may retain chats and coding sessions as required by law»), на англ. Проверено: 2026-10-12.

этого не случится, нет.[166] Анкету придётся заполнить руками, это дольше, чем сфотографировать документ, зато документ остаётся у вас. (☒ 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, удалите каждый такой чат.

Базовый минимум.

1. Откройте список чатов сервиса: он в боковой панели.
2. Удалите по одному каждый чат, где были пароль, документ или чужие данные. Сервис, которым вы не пользуетесь, пропустите.

[166] Claude: используются ли мои данные для обучения моделей и Google: Gemini Apps Privacy Hub, оба на англ. Проверено: 2026-10-12.

- ChatGPT: наведите на чат, нажмите три точки рядом с названием ⊠ «Delete» и подтвердите удаление.[167]
- Claude: наведите на чат, нажмите «⊠» ⊠ «Delete» и ещё раз «Delete» для подтверждения. В приложении на Android: откройте чат ⊠ «⊠» вверху справа ⊠ «Delete». В приложении на iPhone: нажмите на чат в списке и удерживайте ⊠ «Delete» и подтвердите, если приложение попросит.[168]
- Gemini: на gemini.google.com наведите на чат в боковой панели ⊠ «More» ⊠ «Delete». Если список скрыт, нажмите «Menu» вверху. Чат при этом удаляется и из «Gemini Apps Activity».[169]

3. Проверка: в списке не осталось ни одного чата с паролем, документом или чужими данными.

Типовой сбой: нужного чата в списке нет. Удалять нечего, переходите к следующему сервису.

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

> **Максимум**
>
> **Дополнительно: что удаление не отменяет.** Берите, если в удалённых чатах были действительно чувствительные данные. Claude убирает чат из истории сразу, а из своих внутренних систем — в течение 30 дней.[a] ChatGPT планирует окончательное удаление в течение 30 дней, если данные не обезличены заранее и их не нужно хранить по требованию закона или безопасности.[b] Из уже обученной модели данные не убрать.[c] Чаты

[167] OpenAI Help: How to delete and archive chats in ChatGPT, на англ.; страница напрямую не открылась (ответ 403), путь «боковая панель ⊠ три точки ⊠ Delete» взят из пересказа поисковой выдачи по зеркалу этой справки; подтверждения «Delete» в приложении не проверены. Проверено: 2026-10-13.

[168] Claude Help: How can I delete or rename a conversation?, на англ. Проверено: 2026-10-13.

[169] Справка Gemini: удаление чатов и активности, «More» ⊠ «Delete», при удалении чат пропадает и из Gemini Apps Activity; русские подписи кнопок страница не приводит, на англ. Проверено: 2026-10-13.

Gemini, которые уже проверили люди, хранятся отдельно от аккаунта до трёх лет и при удалении активности не стираются.[d] Что отправлено, того не вернуть: поэтому правило выше стоит раньше удаления.

[a] Claude Help: How can I delete or rename a conversation?, «removed from your history immediately and from Anthropic's back-end systems within 30 days», на англ. Проверено: 2026-10-13.

[b] OpenAI Help: How to delete and archive chats in ChatGPT, на англ.; страница напрямую не открылась (ответ 403), срок в 30 дней и исключения взяты из пересказа поисковой выдачи по зеркалу справки. Проверено: 2026-10-13.

[c] Claude: как изменить настройки улучшения моделей, данные, уже вошедшие в обучение, остаются в обученных моделях, на англ. Проверено: 2026-10-13.

[d] Google: Gemini Apps Privacy Hub, чаты, уже просмотренные людьми, не удаляются вместе с активностью и хранятся до трёх лет отдельно от аккаунта, на англ. Проверено: 2026-10-13.

Максимум

Дополнительно (на выбор): отключить обучение на ваших переписках. Берите, если пользуетесь сервисом постоянно. Переключатель отключает только обучение на будущих чатах: уже отправленное он не удаляет, переписка у компании всё равно хранится по её правилам, и сервис он не делает приватным. (☒ защита от утечек).

- Claude: аватар или имя ☒ «Settings» ☒ «Privacy», переключатель про улучшение моделей. Выключенный, он не пускает новые чаты в будущее обучение, но чаты, отмеченные классификаторами безопасности, могут использоваться для безопасности сервиса.[a]
- ChatGPT: «Settings» ☒ «Data controls». Выключение останавливает обучение на новых разговорах, а старые чаты остаются в истории.[b]
- Gemini: «Keep Activity» на странице Gemini Apps Activity (myactivity.google.com/product/gemini). Выключенный, он не пускает будущие чаты в обучение, но Google всё равно хранит их 72 часа.[c]

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

[a] Claude: как изменить настройки улучшения моделей, путь Settings ⊠ Privacy; в поиске и на самой странице название переключателя дано поразному («Help Improve Claude» и «Help Improve our AI models»), поэтому в тексте оно не приводится; на англ. Проверено: 2026-10-13.

[b] OpenAI Help: Data controls in ChatGPT и OpenAI Help: How your data is used to improve model performance, на англ.; страницы напрямую не открылись (ответ 403), путь «Settings ⊠ Data controls» взят из пересказа поисковой выдачи; точная подпись переключателя в тексте не приводится. Проверено: 2026-10-13.

[c] Google: Gemini Apps Privacy Hub, переключатель «Keep Activity» на странице Gemini Apps Activity; при выключении будущие чаты не идут в обучение, но хранятся 72 часа, на англ. Проверено: 2026-10-13.

Проверить ответы чат-бота

Уверенный тон ответа не означает, что ответ правильный. Модель может уверенно сообщить неверное, а тон ответа не показывает, насколько ответ надёжен.[170] Ошибочный ответ нередко звучит так же уверенно, как верный.

Проверяйте всегда, когда в ответе деньги (суммы, реквизиты, тарифы), здоровье (лекарства, дозировки) или официальные бумаги (сроки, штрафы, законы). Остальное, например идеи подарка на день рождения, не проверяйте.

Базовый минимум.

1. Выпишите из ответа конкретное: число, название лекарства, срок, номер статьи.
2. Найдите то же на сайте, который отвечает за это: банка для тарифов и реквизитов, производителя лекарства или инструкцию в упаковке для дозировок, ведомства для сроков и штрафов. *(вывод автора)*
3. Совпало — действуйте. Не совпало или подтверждения нет — верьте сайту, а не боту.

[170] OpenAI Help: Does ChatGPT tell the truth?, на англ.; страница напрямую не открылась (ответ 403), содержание взято из пересказа поисковой выдачи. Проверено: 2026-10-13.

Типовой сбой: подтверждения не нашли. Не действуйте по ответу бота: спросите в банке, у врача или фармацевта. *(вывод автора)*

Получилось — когда каждое число из ответа про деньги, лекарства или документы вы увидели на официальном сайте.

Максимум

Дополнительно (на выбор): локальная модель вместо облачного сервиса. Берите, если конфиденциальность конкретной задачи важнее качества и скорости ответа: юрист с чужими документами, врач с историями болезни, любой, кто по работе регулярно имеет дело с чужими секретами. Для бытовых вопросов (рецепт, письмо) не стоит: обычный веб-сервис с выключенным обучением справится не хуже и без установки, хотя приватность остаётся на условиях компании. Локальные модели, которые тянет обычный домашний компьютер без мощной видеокарты, как правило, слабее и медленнее самых мощных облачных. *(вывод автора)*

По умолчанию берите Ollama: у неё открытый исходный код (лицензия MIT).[a] Пока вы не входите в аккаунт Ollama и не выбираете модели с «cloud» в названии, она, по её FAQ, не видит ваши запросы; облачные модели Ollama обрабатывает у себя.[b]

1. Скачайте Ollama с ollama.com/download. Нужен macOS 14 (Sonoma) или новее, либо Windows 10 22H2 или новее.[c]
2. Установите. Mac: откройте `ollama.dmg` и перетащите Ollama в «Программы» (`/Applications`). Windows: запустите `OllamaSetup.exe`; права администратора не нужны.[d]
3. Откройте терминал (Windows: `cmd` или PowerShell; Mac: приложение «Терминал») и выполните `ollama run gemma4:e2b`. Первый запуск скачивает модель около 7 ГБ, дальше начинается чат прямо в терминале. Выход из чата — `/bye`.[e]
4. Проверка: отключите интернет и задайте вопрос. Ответ пришёл — запрос обрабатывает ваш компьютер. *(вывод автора)*

Памяти должно хватать на файл модели целиком: он загружается в оперативную память или в память видеокарты.[f] Ориентир — 16 ГБ оперативной памяти, как рекомендует LM Studio для Mac и Windows; у Ollama минимум в документации не указан.[g] Если e2b запускается, но отвечает слабо, а памяти хватает, возьмите модель крупнее из той же линейки: `gemma4:12b` — около 8 ГБ, `gemma4:26b` — 16–19 ГБ; чем больше файл, тем больше памяти нужно. Если e2b не запускается из-за нехватки памяти, более крупная модель не запустится тем более: закройте другие программы и повторите шаг 3.[h]

Типовой сбой: команда `ollama` не найдена. Закройте терминал, откройте новый и повторите шаг 3.

Дополнительно (на выбор): LM Studio вместо Ollama. Берите, если не хотите работать в терминале: модели выбираются и запускаются в окне программы. LM Studio бесплатна для дома и работы, но с открытым исходным кодом не распространяется.[i] На Mac нужен процессор Apple Silicon (M1–M4) и macOS 14 или новее; на Windows — x64 с AVX2 или ARM.[j]

---

[a] Ollama на GitHub, лицензия MIT, на англ. Проверено: 2026-10-13.

[b] Ollama FAQ, «We don't see your prompts or data when you run locally»; облачные модели обрабатываются у Ollama, на англ. Проверено: 2026-10-13.

[c] Ollama: macOS и Ollama: Windows, macOS Sonoma (v14) или новее, Windows 10 22H2 или новее, на англ. Проверено: 2026-10-13.

[d] Ollama: macOS и Ollama: Windows, установка `ollama.dmg` в `/Applications`, `OllamaSetup.exe` без прав администратора, на англ. Проверено: 2026-10-13.

[e] Ollama: Quickstart, `ollama run gemma4:e2b`, около 7,2 ГБ загрузки, выход `/bye`, на англ. Проверено: 2026-10-13.

[f] Ollama FAQ, модель загружается в память видеокарты или в оперативную память при работе на процессоре, на англ. Проверено: 2026-10-13.

[g] LM Studio: System Requirements, «16GB+ RAM recommended» для Mac и Windows; для Ollama минимальный объём памяти в документации не указан, на англ. Проверено: 2026-10-13.

[h] Ollama: gemma4, размеры загрузки: e2b 4,6–7,5 ГБ, 12b 7,7–8,0 ГБ, 26b 16–19 ГБ; требований к памяти страница не указывает, на англ. Проверено: 2026-10-13.

[i] LM Studio: free for use at work («free to use both at home and at work») и LM Studio: Terms of Service (исходный код программы — коммерческая тайна, лицензия на личные или внутренние нужды), на англ. Проверено: 2026-10-

13.
[j]LM Studio: System Requirements, Mac: Apple Silicon (M1–M4), macOS 14.0+; Windows: x64 с AVX2 и ARM, на англ. Проверено: 2026-10-13.

Если сводить тему к одной мысли: раньше, чтобы убедительно обмануть, нужно было постараться, а теперь для этого хватает короткой 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, сами по себе блокировщик и настройки приватности редко решают исход такой истории. *(вывод автора)* 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
- ☐ Поставить VPN и подключиться — 5 минут

Поставить блокировщик рекламы

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.

Реклама с сомнительными баннерами и всплывающими окнами перестаёт показываться, а вместе с ней отсекается и часть вредоносной рекламы (malvertising), через которую иногда пытаются подсунуть что-нибудь неприятное даже на обычном сайте. Защи-

той от вредоносных файлов блокировщик при этом не является. А трекеры — небольшие невидимые скрипты, которые следят, на какие сайты вы заходите, и складывают эту историю в рекламный профиль, — просто перестают загружаться, и страницы обычно открываются быстрее. Стопроцентной гарантии блокировщик не даёт: часть рекламы и трекеров всё равно просачивается, особенно там, где сайт специально борется с блокировщиками. *(вывод автора)* (☒ цифровой след после посещений).

Правило выбора одно для всей темы: сначала программа с открытым исходным кодом, потом бесплатная, потом самая популярная. По нему блокировщик — uBlock Origin: код открыт (лицензия GPLv3), он бесплатный, а каталог расширений Firefox отмечает его значком «Recommended».[171]

Базовый минимум.

1. Откройте браузер, которым пользуетесь чаще всего. Если выбираете браузер сами, берите Firefox: его исходный код открыт.[172] Браузеров с открытым кодом несколько, Firefox выбран автором: сравнения по популярности здесь нет. *(вывод автора)*
2. Поставьте блокировщик для своего браузера. Ссылки на магазины взяты с официальной страницы проекта uBlock Origin Lite.[173]
    - Firefox: откройте страницу uBlock Origin, нажмите «Add to Firefox» и подтвердите установку в окне с запросом разрешений.[174]
    - Chrome: полную uBlock Origin из Chrome Web Store убрали,[175] поэтому откройте uBlock Origin Lite и нажмите

[171] Firefox Add-ons: uBlock Origin, лицензия GPLv3, значок «Recommended», на англ. Проверено: 2026-10-13.

[172] Mozilla: Firefox terms of use, «We make the source code for Firefox available to you under the terms of various open source licenses», на англ. Проверено: 2026-10-13.

[173] uBlock Origin Lite: официальная страница проекта, ссылки на Chrome Web Store, Edge Add-ons и App Store, на англ. Проверено: 2026-10-13.

[174] Mozilla Support: Use extensions to add features to Firefox, кнопка «Add to Firefox», на англ. Проверено: 2026-10-13.

[175] uBlock Origin: README проекта, в Chrome Web Store «Removed on 2026-08-31», на англ. Проверено: 2026-10-13.

«Add to Chrome».[176]

- Edge: откройте uBlock Origin Lite в Edge Add-ons, нажмите «Get», затем «Add extension».[177]
- Safari на Mac: откройте uBlock Origin Lite в App Store (бесплатно, нужна macOS 13.5 или новее)[178] и поставьте приложение. Затем выберите в Safari Safari ⊠ Settings ⊠ Extensions и отметьте галочкой uBlock Origin Lite.[179]
- Яндекс Браузер: нажмите значок расширений в правом верхнем углу, затем «Добавить расширение», откройте в каталоге Chrome страницу uBlock Origin Lite, нажмите кнопку установки на странице расширения и подтвердите установку после списка данных, к которым расширение получит доступ.[180]

3. Откройте любой привычный сайт с рекламой. Результат: баннеры и всплывающие окна исчезли без дополнительных настроек.

Если сайт без рекламы не работает: нажмите значок блокировщика и отключите его для этого сайта. В uBlock Origin это большая кнопка включения, она отключает блокировщик для текущего сайта;[181] в uBlock Origin Lite выберите в том же окне другой режим фильтрации: в справке проекта названы режимы «Optimal» и «Complete».[182] Какой из них снимет поломку, зависит от сайта. Затем перезагрузите страницу. *(вывод автора)*

---

[176] Chrome Web Store Help: Install and manage extensions, кнопка «Add to Chrome», на англ. Проверено: 2026-10-13.

[177] Microsoft: Add, turn off, or remove extensions in Microsoft Edge, кнопки «Get» и «Add extension», на англ. Проверено: 2026-10-13.

[178] App Store: uBlock Origin Lite, бесплатно, macOS 13.5 или новее, на англ. Проверено: 2026-10-13.

[179] Apple: Safari Extensions on Mac, включение через Safari ⊠ Settings ⊠ Extensions, на англ. Проверено: 2026-10-13.

[180] Справка Яндекс Браузера: Расширения, установка из каталога: значок расширений, «Добавить расширение», подтверждение установки; поддерживаются каталоги Chrome и Opera, на рус. Проверено: 2026-10-13.

[181] uBlock Origin wiki: Quick guide, popup user interface, большая кнопка включения отключает uBO для текущего сайта, на англ. Проверено: 2026-10-13.

[182] uBlock Origin Lite: FAQ проекта, режимы «Optimal» и «Complete», на англ. Проверено: 2026-10-13.

Максимум

Дополнительно (на выбор).

Полная uBlock Origin в Edge — выбирайте, если вам нужны её расширенные возможности, а не простота Lite. Сейчас она есть в Edge Add-ons, но Microsoft ставит целью завершить переход Edge на Manifest V3 к концу 2026 года, так что её доступность может измениться.[a]

[a] uBlock Origin: README проекта, цитата Microsoft: «Our goal is to complete the consumer transition by the end of 2026», на англ. Проверено: 2026-10-13.

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

Сменить поисковик по умолчанию

Многие поисковики по умолчанию сохраняют историю запросов, связанную с аккаунтом или устройством; есть и такие, вроде DuckDuckGo, которые по своей политике не сохраняют IP-адрес рядом с запросами.[183] Среди таких поисковиков берём DuckDuckGo: он зарабатывает на рекламе в поиске, а не на ваших данных,[184] и по данным самой компании обрабатывает около 3 миллиардов поисковых запросов в месяц.[185] (☒ метаданные).

Базовый минимум.

1. Откройте настройки поиска своего браузера (названия пунктов даны по английскому интерфейсу, в русском подписи могут отличаться; для Яндекс Браузера — по русскому):
    - Chrome: три точки ☒ Settings ☒ Search engine, рядом с «Search engine» нажмите «Change».[186]

[183] DuckDuckGo: политика приватности, на англ. Проверено: 2026-10-11.

[184] DuckDuckGo: About, «We make money from privacy-respecting search ads, not by exploiting your data», на англ. Проверено: 2026-10-13.

[185] DuckDuckGo: About, страница называет 3B monthly searches, на англ. Проверено: 2026-10-13.

[186] Google Chrome Help: Change your default search engine, Settings ☒ Search engine

- Firefox: Settings ⊠ Search, список «Default Search Engine».[187]
- Safari на Mac: Safari ⊠ Settings ⊠ Search, пункт «Search engine».[188]
- Edge: три точки ⊠ Settings ⊠ Privacy, search, and services ⊠ Search and connected services ⊠ Address bar and search, список «Search engine used in the address bar».[189]
- Яндекс Браузер: нажмите правой кнопкой мыши Умную строку, выберите «Управление поисковыми системами...», на странице «Настройки поисковой системы» в разделе «Поисковая система по умолчанию» выберите нужный вариант из списка.[190]

2. Выберите DuckDuckGo.
3. Введите в адресной строке любое слово. Результат: страница результатов на duckduckgo.com.

Если DuckDuckGo нет в списке выбора — шаг пропустите, остальная тема от него не зависит. *(вывод автора)*

> **Максимум**
>
> **Дополнительно (на выбор).**
>
> *Отдельный профиль браузера — выбирайте, если устройством пользуются несколько человек или хочется держать работу отдельно.* Второй профиль — это отдельное окно со своими закладками, паролями и историей, а не отдельная программа. В Chrome и Edge он заводится через значок профиля справа от

⊠ Change, на англ. Проверено: 2026-10-13.

[187] Mozilla Support: Manage Firefox search settings, Settings ⊠ Search ⊠ Default Search Engine, на англ. Проверено: 2026-10-13.

[188] Apple: Change Search settings in Safari on Mac, Safari ⊠ Settings ⊠ Search, на англ. Проверено: 2026-10-13.

[189] Microsoft Support: Change your default search engine in Microsoft Edge, Settings ⊠ Privacy, search, and services ⊠ Search and connected services ⊠ Address bar and search, на англ. Проверено: 2026-10-13.

[190] Справка Яндекс Браузера: Настройки поиска, «Управление поисковыми системами...», «Настройки поисковой системы», «Поисковая система по умолчанию», на рус. Проверено: 2026-10-13.

адресной строки, в Firefox — через about:profiles. Входите из него в магазины и разовые регистрации.

Второй почтовый адрес — выбирайте, если часто регистрируетесь на сайтах. Заведите два адреса: один под по-настоящему важное — банк, сайты госсервисов, рабочую переписку, восстановление доступа к другим аккаунтам; второй под всё остальное — регистрации в магазинах, рассылки, форумы. Рано или поздно база какого-нибудь магазина утечёт вместе с адресом и, возможно, паролем. Если утечёт «магазинный» адрес, по нему разве что придёт спам, а главный адрес в этой утечке не окажется.

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

Чистка данных сайтов — выбирайте, если браузер давно не чистили. Раз в 3 месяца стирайте куки и данные сайтов в настройках браузера, в разделе про приватность. *(вывод автора)* Потеряете вы немного — придётся заново войти на паре сайтов, — зато исчезнет хвост данных, которые уже никому не нужны, кроме тех, кто их собрал. (☒ следы браузера). Точный путь в меню зависит от браузера и версии.

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

Выбрать защищённую 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. Шифрование соединения до сервера само по себе не делает такую переписку сквозной.[191]

Базовый минимум.

1. 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. Паспорт и данные карты не пересылайте вообще никак, в том числе в Signal; пароли передавайте только голосом (шаг 2).
2. Пароли храните в KeePassXC. Если пароль нужно передать один раз, назовите его голосом при встрече или по звонку на номер из ваших контактов, а потом смените. *(вывод автора)*
3. Для обычной переписки поставьте Signal по шагам ниже.

Установить Signal

Сквозное шифрование — фраза, которую мессенджеры вставляют в рекламу так часто, что она почти перестала что-либо значить, а смысл простой: прочитать переписку не может даже компания, которой принадлежит мессенджер. Ключи для расшифровки хранятся только на устройствах участников разговора, а на серверах компании переписка лежит нечитаемым набором символов. Защита скрывает содержимое, но не сам факт переписки (кто и когда), и не мешает собеседнику сделать скриншот и переслать его дальше.

Signal выбран по тому же правилу: код открыт, приложение бесплатное, а сквозное шифрование в нём включено для всех пере-

[191] Telegram FAQ: облачные чаты используют шифрование клиент-сервер, не сквозное, на англ. Проверено: 2026-10-11.

писок без исключения и не требует настройки.[192] В других приложениях оно бывает только в отдельном режиме для конкретного собеседника, а то и вовсе отсутствует.

Базовый минимум.

1. Установите Signal из магазина приложений своего телефона (App Store или Google Play) и зарегистрируйтесь по номеру телефона. Номер нужен для регистрации, но анонимным Signal он не делает.[193]
2. Откройте Settings / Настройки ⊠ Account / Аккаунт, задайте Signal PIN / Signal PIN (не короче 4 цифр; можно длиннее или с буквами)[194] и сразу сохраните его в KeePassXC. Включите Registration Lock / Блокировка регистрации.
3. Откройте Settings / Настройки ⊠ Privacy / Конфиденциальность и включите Screen Lock / Блокировка экрана.
4. Напишите в Signal одному человеку, у которого он установлен. Результат: ваше сообщение появилось в чате с ним.
5. Раз в месяц открывайте Linked Devices / Связанные устройства и отключайте незнакомые. *(вывод автора)*

Забыли PIN при включённой блокировке регистрации: блокировка истекает только после 7 дней неактивности аккаунта, так что PIN в менеджере паролей — не формальность.[195]

> **Максимум**
>
> **Дополнительно (на выбор).**

[192] Signal: сквозное шифрование всегда включено, это не опциональный режим, на англ. Проверено: 2026-10-11.

[193] Signal: для регистрации по-прежнему нужен номер телефона, на англ. Проверено: 2026-10-11.

[194] Signal: Introducing Signal PINs, «at least 4 digits, but they can also be longer or alphanumeric», на англ. Проверено: 2026-10-13.

[195] Signal Support: Signal PIN, блокировка регистрации истекает после 7 дней неактивности, на англ. Проверено: 2026-10-13.

Signal

Код безопасности — выбирайте для тех, с кем обсуждаете деньги или документы. 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 личность собеседника не доказывает.

Исчезающие сообщения — выбирайте, если хотите автоматически чистить историю. Они не защищают от скриншота, фотографии экрана, копирования текста или записи другим устройством. Таймер для новых чатов задаётся в `Settings` / `Настройки` ⊠ `Privacy` / `Конфиденциальность` в пункте «Default timer for new chats»; есть варианты от 30 секунд до 4 недель.[a] Начните с 1 недели. *(вывод автора)*

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

Telegram: секретный чат

Выбирайте, если нужен именно Telegram и содержание личного разговора должно быть E2EE. Откройте профиль контакта, меню (три точки) и выберите `Start Secret Chat` / `Начать секретный чат`. Убедитесь, что чат помечен как Secret Chat, а не является обычным облачным. 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 и не защищает группы, каналы и обычные чаты. Он привязан к устройствам, на которых его начали, и не синхронизируется как облачная переписка.[b] Он защищает содержимое сообщений; сведения о том, что вы пользуетесь Telegram (аккаунт, номер, IP), не скрывает. *(вывод автора)* Предупреждение о скриншоте не гарантия: экран можно сфотографировать другим устройством или обойти такое предупреждение.

E2EE защищает канал от перехвата, но не от получателя, разблокированного или заражённого телефона.

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

Session

Выбирайте, если важна регистрация без номера телефона и допустимы псевдонимность и задержки доставки. Session не требует номера или почты.[c] (⊠ обзор Session). 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 в запертом ящике дома, не в облаке и не в фото; никому её не сообщайте. *(вывод автора)* 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 протокол V1 не даёт Perfect Forward Secrecy; её вернёт Session

Protocol V2, он пока в разработке.[d] (⊠ 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.

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 в запертый ящик; 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 Session, сохранить секрет восстановления вне чата и проверить одного собеседника через второй канал.

[a] Signal Support: Set and manage disappearing messages, Settings ⊠ Privacy ⊠ Default timer for new chats, до 4 недель, на англ. Проверено: 2026-10-13.

[b] Telegram FAQ: секретные чаты только между двумя людьми, привязаны к устройствам и не входят в облако Telegram, на англ. Проверено: 2026-10-11.

[c] Session FAQ: не требует ни номера телефона, ни почты, на англ. Проверено: 2026-10-11.

[d] Session: как устроен протокол (V1 без Perfect Forward Secrecy, V2 в разработке), на англ. Проверено: 2026-10-11.

	Signal	Session
Номер и почта	Нужен номер для регистрации	Не нужны
Идентификатор	Номер телефона (по умолчанию не виден всем, с кем вы общаетесь)[e] или имя пользователя (username)	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
Критерий выбора	Базовый вариант для проверенных контактов	Нужна регистрация без номера, допустимы псевдонимность и задержки

> Критерий выбора: нужна регистрация без номера — Session; нужен именно Telegram — его секретный чат; во всех остальных случаях — Signal. Правило общее для всех: паспорт и данные карты не пересылать вообще, пароли передавать только голосом.

Проверить страницу в соцсети

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. Это не для того, чтобы ужаснуться, а взгляд в зеркало заднего вида: вы увидите то, что там уже давно видят все, кроме вас самих.

Базовый минимум.

1. Откройте свой профиль в соцсети и скопируйте адрес страницы из адресной строки.
2. Откройте приватное окно браузера (через меню браузера), не заходя в аккаунт. Вставьте скопированный адрес.
3. Проверьте четыре вещи и выпишите те, что видны: телефон, список друзей целиком, старые фотографии за прошлые годы, место работы.
4. Для каждой выписанной вещи вернитесь в свой аккаунт, откройте настройки приватности соцсети и ограничьте аудиторию до «Только друзья». Если такого варианта нет — выберите «Только я» или уберите сведения из профиля. В Facebook это: Settings & privacy ⊠ Settings ⊠ Privacy, дальше «Friends» или «Only me» для нужной вещи.[196] В Instagram «друзей» нет: Settings and activity ⊠ Account privacy ⊠ Private account.[197] Названия пунктов зависят от сети и от языка интерфейса, в других сетях ищите раздел про приватность и аудиторию. *(вывод автора)*
5. Повторите шаги 2–3. Результат: из четырёх вещей посторон-

[196]Facebook Help Center: настройки приватности, Settings & privacy ⊠ Settings ⊠ Privacy, варианты «Friends» и «Only me», на англ. Проверено: 2026-10-13.

[197]Instagram Help Center: сделать аккаунт закрытым, Settings and activity ⊠ Account privacy ⊠ Private account, на англ. Проверено: 2026-10-13.

ним видно только то, что вы оставили видимым сами.

Если настройки нужной вещи нет — удалите её из профиля: что не опубликовано, того не увидит никто. *(вывод автора)*

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

Максимум

Дополнительно (на выбор).

Попросить знакомого посмотреть вашу страницу — выбирайте, если у вас нет приватного окна под рукой или страница видна только залогиненным. Пусть он откроет вашу страницу со своего аккаунта и перечислит то, что видит.

Убрать старые следы — выбирайте, когда хотите почистить не только соцсеть. Полный список того, где ваше имя и фотография уже когда-то засветились, обычно длиннее, чем кажется: старый форум, комментарий пятилетней давности под чужим постом, профиль на сайте, которым вы пользовались один раз. Действуйте по порядку: сначала удалите аккаунт через настройки самого сервиса; нет такой кнопки — напишите в поддержку сервиса с просьбой удалить аккаунт; отдельный пост на форуме — попросите владельца форума стереть его. Часть убрать не удастся: 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 гнаться за ней не нужно. *(вывод автора)* Достижимая цель скромнее — убрать то, что явно лишнее и давно не нужно: не «обо мне в сети ничего нет», а «там нет того, чего там быть не должно».

Включить VPN

VPN стоит поставить каждому: он прячет ваш исходящий трафик от провайдера интернета и от владельца сети, в которой вы сидите, — кафе или гостиницы. Это не плащ-невидимка: наблюдателя он не убирает, а заменяет. Провайдер интернета больше не видит ваших сайтов, зато их целиком видит провайдер VPN.[198]

Правило выбора то же: сначала открытый код, потом бесплатный. По нему VPN — Proton VPN: код его приложений открыт,[199] есть бесплатный тариф без лимита трафика и времени,[200] а политику без логов проверил независимый аудитор.[201]

Про доверие. Провайдер VPN видит всё, что раньше видел провайдер интернета, поэтому доверие здесь решает. Выбирайте проверяемого: у него открыт код приложений, который могут изучить посторонние *(вывод автора)*, и независимые аудиты публикуют результаты. Обещание «мы не храним логи» одно ничего не гарантирует, а недобросовестный сервис способен собирать ваши данные.[202]

Базовый минимум.

1. Откройте protonvpn.com/download и скачайте приложение для своего устройства: официальные приложения есть для Windows, macOS, Android, iOS и Linux.[203] На телефоне проще

[198] EFF Surveillance Self-Defense: Choosing the VPN That's Right for You, «A VPN also hides your outgoing traffic from your ISP and the local network owner (like a coffee shop or hotel)» и «while a VPN hides your browsing data from the ISP, it's all visible to the VPN provider», на англ. Проверено: 2026-10-13.

[199] Proton VPN: All Proton VPN apps are now open source and audited, открытый код приложений для Windows, macOS, Android и iOS, на англ. Проверено: 2026-10-13.

[200] Proton VPN: Free VPN, «Has no data or speed limits», «Has no advertisements», на англ. Проверено: 2026-10-13.

[201] Proton VPN passes 5th annual external audit of no-logs policy, аудит фирмы Securitum, на англ. Проверено: 2026-10-13.

[202] EFF Surveillance Self-Defense: Choosing the VPN That's Right for You, «Do not use a VPN that you do not trust», аудиты третьих сторон с публикуемыми результатами, «Even if a company claims not to log connection data, this is not a guarantee of good behavior», на англ. Проверено: 2026-10-13.

[203] Proton VPN: Download, приложения для Windows, macOS, Android, iOS и Linux, на англ. Проверено: 2026-10-13.

поставить приложение из магазина: App Store на iPhone[204] или Google Play на Android.[205]

2. Откройте приложение и создайте бесплатный аккаунт: в приложении для Windows это кнопка «Create Account».[206] Бесплатный тариф рассчитан на одно устройство,[207] поэтому ставьте VPN на то, которым чаще пользуетесь вне дома. *(вывод автора)*
3. Войдите в аккаунт и нажмите кнопку подключения. В приложении для Windows она называется «Connect» и подключает к самому быстрому бесплатному серверу,[208] в приложениях для macOS, Android и iOS — «Quick Connect».[209][210][211]
4. Результат: приложение показывает, что вы подключены. Откройте любой сайт — он должен открыться как обычно.

Если подключиться не получилось: закройте приложение, откройте его заново и нажмите кнопку подключения ещё раз. *(вывод автора)*

> **Максимум**
>
> **Дополнительно (на выбор).**
>
> *Mullvad VPN — выбирайте, если готовы платить и хотите*

[204] Proton VPN: Download VPN for iPhone and iPad, «Download and install Proton VPN from the App Store», на англ. Проверено: 2026-10-13.

[205] Proton VPN: Download VPN for Android, «The easiest way to install our app is from the Play Store», на англ. Проверено: 2026-10-13.

[206] Proton VPN: How to use the Proton VPN app for Windows, кнопка «Create Account», на англ. Проверено: 2026-10-13.

[207] Proton VPN: Free VPN, бесплатный тариф: «1 device», на англ. Проверено: 2026-10-13.

[208] Proton VPN: How to use the Proton VPN app for Windows, «select Connect to automatically connect to the fastest free server for your location», на англ. Проверено: 2026-10-13.

[209] Proton VPN: How to use the Proton VPN macOS app, «To immediately connect to a VPN server, click the Quick Connect button», на англ. Проверено: 2026-10-13.

[210] Proton VPN: Download VPN for Android, «touch the Quick Connect button at the bottom right of your screen», на англ. Проверено: 2026-10-13.

[211] Proton VPN: Download VPN for iPhone and iPad, «touch the Quick Connect button at the bottom center of your screen», на англ. Проверено: 2026-10-13.

приложение, прошедшее независимые аудиты. Стоит €5 в месяц, бесплатного тарифа нет.[a] Все пять платформенных версий приложения в 2020 году прошли внешний аудит безопасности;[b] код приложения открыт под лицензией GPLv3.[c]

RiseupVPN — выбирайте, если не хотите заводить аккаунт. Не требует настройки и регистрации аккаунта, живёт на пожертвования и просит около 60 долларов США в год с человека.[d]

Платный тариф Proton VPN — выбирайте, если VPN нужен на нескольких устройствах. Платные тарифы позволяют подключить до 10 устройств.[e]

[a] Mullvad VPN: Pricing, €5 в месяц, бесплатного плана нет, на англ. Проверено: 2026-10-13.

[b] Mullvad VPN: About, июнь 2020: «All five platform versions of our VPN app underwent a thorough external security audit», на англ. Проверено: 2026-10-13.

[c] Mullvad VPN: исходный код приложения, лицензия GNU GPL версии 3, на англ. Проверено: 2026-10-13.

[d] Riseup: RiseupVPN, «no configuration, no account registration», финансируется пожертвованиями, около 60 долларов США в год на человека, на англ. Проверено: 2026-10-13.

[e] Proton VPN: Free VPN, платные тарифы: «Up to 10 devices», на англ. Проверено: 2026-10-13.

Подключаться к публичному Wi-Fi

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 все сайты, которые вы открываете, и так используют HTTPS, и просто перехватить данные из воздуха стало заметно труднее, чем раньше *(вывод автора)* (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: поддельная точка доступа с похожим названием или страница-заглушка, которая просит «войти в сеть» и вместо простой авторизации спрашивает пароль от настоящей почты.

Базовый минимум.

1. На публичном Wi-Fi банк и почту не открывайте: переключитесь на мобильный интернет на те минуты, что нужны для входа, а к Wi-Fi вернитесь потом, для всего остального.
2. Заходите в банк и почту только из их приложения или из своей закладки — не по ссылке из письма и не по форме, которую подсунула сама сеть.
3. Пароль от почты на странице входа в Wi-Fi не вводите никогда. Если заглушка просит именно пароль, а не просто адрес почты, отключитесь от этой сети.

Если не получилось. Мобильного интернета нет — включите VPN из раздела выше до того, как откроете банк или почту: он не заменяет шаги 2–3. *(вывод автора)*

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. Переключиться на мобильный интернет и 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: мобильный интернет и вход своим путём. VPN включать стоит, но он 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, VPN, взгляд на собственную страницу со стороны и один осмысленный разговор про мессенджер закрывают львиную долю того, что вообще можно закрыть за двадцать 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

Выбрать, откуда скачать программу

Программа попадает на устройство разными путями, и они далеко не равноценны. Правило одно, для любой программы: сначала встроенный магазин приложений, потом официальный сайт разработчика, а случайная ссылка из поиска — никогда. Если в одной категории подходит несколько программ, берите по порядку: у которой открытый исходный код, потом бесплатную, потом ту, которой больше всего пользуются.

Базовый минимум.

1. Откройте магазин приложений вашей системы (App Store, Google Play, Microsoft Store, магазин на Mac) и найдите программу по названию. Нашли — ставьте оттуда и дальше

не ищите. Площадка проверяет публикуемое и может убрать программу после выпуска, но это не гарантия: вредоносные приложения в магазинах тоже встречаются.*(вывод автора)* Типовой сбой: в магазине несколько программ с похожим названием — берите ту, у которой имя разработчика совпадает с официальным сайтом.*(вывод автора)*

2. Нет в магазине — ставьте с официального сайта разработчика. Адрес берите не из поиска: откройте статью о программе в Википедии и перейдите по ссылке на официальный сайт из карточки справа.*(вывод автора)* Статьи нет — в результатах поиска пропускайте всё с рекламной пометкой «Ads»[212] и открывайте только тот результат, чей адрес совпадает с названием разработчика.
3. Нет ни в магазине, ни на сайте — не ставьте. Возьмите открытый аналог из списка в следующем разделе.

Почему не по первой ссылке из 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. Так, поддельные 7-Zip, Notepad++ и Office продвигали через рекламу в поиске с захваченных рекламных аккаунтов Google (кампания была нацелена на пользователей Mac).[213] Поэтому поймать вредонос можно не открывая подозрительный файл специально, а просто нажав на первую ссылку в поиске, не заметив, что это реклама, а не результат.

Если программа уже стоит и вы не помните, откуда она.

1. Android: Google Play ☒ значок профиля ☒ «Управление приложениями и устройством» ☒ «Управление».[214] Программа в списке — источник Google Play.
2. Остальные системы: найдите программу в магазине по названию. Магазин показывает её как установленную — источник

[212] Справка Google Рекламы: где показываются объявления, на англ.; объявления в поиске показываются под пометкой «Ads». Проверено: 2026-10-13.

[213] Bitdefender: угнанные рекламные аккаунты Google продвигают поддельные 7-Zip, Notepad++ и Office, на англ.; источник описывает кампанию против пользователей Mac, а не поиск в целом. Проверено: 2026-10-12.

[214] Справка Google: удаление приложений. Проверено: 2026-10-11.

магазин.*(вывод автора)*
3. Источник найти не удалось — удалите программу и поставьте заново по трём шагам выше.

Максимум

Дополнительно (на выбор).

Репозиторий — выбирайте, если хотите, чтобы программы обновлялись сами, пачкой. Репозиторий — открытый каталог программ: устройство подключается к каталогу целиком, а дальше все программы из него обновляются вместе, без отдельного скачивания. Это в первую очередь история Linux и Android, а не универсальный способ на все системы сразу.

- Linux: программы ставятся через магазин приложений дистрибутива (например, GNOME Software, «Центр приложений» в Ubuntu) — обычное окно со списком и кнопкой «Установить», терминал не нужен.
- Android без Google Play: F-Droid — каталог программ с открытым кодом, из которого их можно ставить без магазина Google.[a] Автообновление на Android 12 и новее включается в настройках F-Droid.[b]
- Windows и Mac: магазин приложений — ближайший аналог репозитория. Для продвинутых пользователей есть менеджеры пакетов: в Windows — winget (`winget install имя-программы`),[c] на Mac — Homebrew (`brew install имя-программы`).[d]

Разница с обычным скачиванием не в удобстве, а в устройстве 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 через каталог, вместе со всем остальным, что стоит рядом, и каждый раз приходит из одного и того же проверенного места.

Источник через историю загрузок — если магазин источник не показал. Многие браузеры в истории загрузок показывают ад-

рес, с которого скачан файл, но только если программа вообще пришла через браузер. Android не везде показывает, из какого магазина поставлено приложение: это зависит от версии системы и оболочки производителя.

[a] F-Droid, на англ. Проверено: 2026-10-11.

[b] F-Droid: новости, версия 1.19.0, на англ.; автообновление на Android 12 и новее включается в настройках F-Droid, точное название пункта источник не называет. Проверено: 2026-10-13.

[c] Microsoft Learn: WinGet, на англ.; подтверждает команду `winget install` и открытый код. Проверено: 2026-10-13.

[d] Homebrew, на англ.; подтверждает менеджер пакетов для macOS и команду `brew install`. Проверено: 2026-10-13.

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 помогает с обновлениями.

Первый, третий и четвёртый. Основной порядок такой: магазин, потом официальный сайт; каталог программ — дополнительный путь. 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».

Распознать ловушку «скачать бесплатно»

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. *(вывод автора)*

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.

Базовый минимум.

1. Взломанную версию не ставьте никогда.
2. Найдите в списке свою платную программу и поставьте её бесплатный аналог с открытым кодом по шагам из первого раздела:
   - вместо Microsoft Office — LibreOffice;[215]
   - вместо Photoshop — GIMP;[216]
   - вместо платного проигрывателя видео — VLC;[217]
   - вместо платного архиватора — 7-Zip: бесплатный, исходный код выложен на GitHub. Официальные ссылки на него ведут на страницу релизов проекта на GitHub (github.com/ip7z/7zip) — это нормально и ожидаемо, а не подмена.[218]
3. Вашей программы в списке нет — найдите аналог поиском

[215] LibreOffice: о проекте, на англ.; офисный пакет с открытым кодом. Проверено: 2026-10-13.

[216] GIMP, на англ.; «The Free & Open Source Image Editor». Проверено: 2026-10-13.

[217] VideoLAN: VLC, на англ.; «a free and open source cross-platform multimedia player». Проверено: 2026-10-13.

[218] 7-Zip: страница загрузки, на англ.; страница ведёт на релизы проекта на GitHub и ссылку на исходники. Проверено: 2026-10-13.

«имя программы open source alternative», но результаты с пометкой «Ads» пропускайте.*(вывод автора)*

4. Аналога нет, а платить нечем — берите бесплатную урезанную версию у самого разработчика, с его официального сайта.

Если в категории несколько подходящих программ, порядок выбора тот же: открытый код, бесплатная, самая популярная. Из списка выше так выбраны LibreOffice, GIMP, VLC и 7-Zip. Где открытых бесплатных аналогов несколько, «самая популярная» — оценка автора, а не измерение по источникам. *(вывод автора)*

Оценить открытый код

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, повышает шанс, что подлость заметят: её может увидеть кто-то из тех независимых людей, которые время от времени читают чужой код, — энтузиасты, исследователи безопасности, конкуренты. *(вывод автора)* Гарантии нет: проверка происходит, только если кто-то реально смотрит. У закрытой программы такого открытого просмотра нет: код видят автор и те, кого он сам туда допустил, — например, аудитор по контракту, — а не любой желающий со стороны.

Базовый минимум. Есть открытый аналог из магазина — берите его. Нет — ставьте закрытую программу из магазина или с официального сайта. Отказываться от закрытой программы только за то, что она закрытая, не нужно: у открытости 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).

Сверить контрольную сумму

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.

Сверяйте сумму у файлов, скачанных с сайта, а не из магазина, если программа требует прав администратора или ставится надолго на основное устройство. Для программы, которой вы воспользуетесь один раз, сверка не обязательна. (⊠ как подойти к аудиту программы).

Базовый минимум.

1. Найдите на странице скачивания строку «SHA-256» рядом со ссылкой. Строки нет — сверять нечего: возьмите программу из магазина или выполните шаги 2–3, пропустите 4–5 и перейдите к шагам 6–7.
2. Откройте терминал. Windows: «Пуск», введите Windows PowerShell, выберите Windows PowerShell и нажмите «Открыть» (Open).[219] Mac: найдите программу «Терминал» через поиск Spotlight.*(вывод автора)*
3. Вычислите сумму скачанного файла штатной командой:
    - Mac: введите `shasum -a 256` (с пробелом на конце), перетащите файл из Finder в окно «Терминала» — путь подставится сам[220] — и нажмите Return.*(вывод автора)*

[219]Microsoft Learn: запуск Windows PowerShell, на англ.; открыть меню «Пуск», ввести Windows PowerShell, выбрать его и нажать «Open». Проверено: 2026-10-13.

[220]Поддержка Apple: перетаскивание объектов в окно «Терминала», на англ.; путь к файлу подставляется в командную строку. Проверено: 2026-10-13.

- Windows: введите `cd Downloads` и нажмите Enter (файл лежит в папке «Загрузки», если вы не меняли её),*(вывод автора)* затем `certutil -hashfile имя-файла SHA256`.[221]
- Linux: в терминале перейдите в папку с файлом и выполните `sha256sum имя-файла`.*(вывод автора)*

4. Сравните результат со строкой на сайте: она должна совпасть полностью, буква в букву.
5. Совпало — ставьте. Не совпало — удалите файл и скачайте заново; не совпало и во второй раз — не устанавливайте. (☒ проверка контрольной суммы).
6. Затем вставьте ту же сумму в строку поиска на сайте VirusTotal — бесплатной публичной проверки файла или ссылки сразу многими антивирусными движками.[222] Сайт принимает суммы SHA-256, MD5 и SHA1 и показывает последний отчёт, если файл кто-то уже проверял до вас. Такой поиск не раскрывает сам файл, в отличие от его загрузки.*(вывод автора)* Отчёта нет (хэш никто не проверял) — это не значит, что файл чист: возьмите программу из магазина или найдите другой источник.*(вывод автора)*
7. Читайте результат так: 0 срабатываний — ставьте; 1–2 срабатывания у малоизвестной программы — не запускайте и найдите другой источник; 1–2 у известной программы (её выпускает крупный разработчик, скачана с его официального сайта) — сверьте отчёт по второму источнику (другой хэш на сайте разработчика) и, если расхождений нет, считайте ложным; 3 и больше — удалите файл.*(вывод автора)* Единичное срабатывание может быть ложным.

Типовой сбой: строки не совпали у честного файла — выбран не тот алгоритм или не та версия файла. Проверьте, что в команде SHA-256 (как на сайте) и что скачана именно та версия, чей хэш вы сверяете.

Если macOS показывает предупреждение Gatekeeper, не отключай-

[221] Microsoft Learn: certutil, на англ.; подтверждает только команду для Windows, `shasum` и `sha256sum` этим источником не подкреплены. Проверено: 2026-10-12.

[222] Документация VirusTotal: поиск, на англ.; поиск принимает MD5, SHA1 и SHA256 и показывает последний отчёт. Проверено: 2026-10-13.

те его и не выбирайте «Все равно открыть» просто для продолжения.[223] Закройте окно предупреждения, удалите файл и скачайте заново с официального сайта.*(вывод автора)*

Максимум

Дополнительно (на выбор).

QuickHash-GUI — если не хотите работать в терминале. Это 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 (например, SHA-256), 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 `Expected Hash Value` / `Ожидаемое значение хэша`: можно вставить в него строку с сайта, и программа сама сравнит две суммы.*(вывод автора)* Названия вкладки и поля взяты из английского интерфейса программы и в официальных описаниях проекта не приведены; если у вас они выглядят иначе, ищите вкладку для одного файла и поле для эталонной суммы.

Телефон — если файл скачан прямо на 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; в ЕС, Японии и Бразилии Apple разрешает и альтернативные магазины, в остальных странах — нет.[a] Для Android берите DeadHash: открытый исходный код (лицензия GPL-3.0),

[223] Поддержка Apple: открытие программ на Mac с предупреждением Gatekeeper. Проверено: 2026-10-11.

ставится из F-Droid, исходники лежат на GitHub. Считает SHA-256, а заодно MD5, SHA-1, SHA-512 и другие.[b] Порядок работы: скачанный файл должен лежать в памяти телефона.

1. Откройте F-Droid, найдите в нём «DeadHash» и нажмите установку.*(вывод автора)*
2. Откройте DeadHash и выберите скачанный файл.*(вывод автора)*
3. Выберите алгоритм, тот же, что назван на сайте рядом со ссылкой (например, SHA-256).*(вывод автора)*
4. Сравните полученную строку со строкой на сайте: она должна совпасть полностью.

Названия кнопок в DeadHash официальные страницы не приводят, поэтому они здесь не указаны.*(вывод автора)*

Приложение поддерживается и обновлялось в течение последнего года.[c] Если DeadHash устареет, ищите замену по двум признакам: последнее обновление в карточке приложения старше двух лет — не берите, и приложение просит доступ к контактам, геолокации или чему-то ещё за пределами файлов — не берите.*(вывод автора)*

VirusTotal: загрузка файла — запасной вариант, если поиск по сумме ничего не нашёл. Содержимое загруженных файлов может стать доступно платным клиентам VirusTotal, а результаты проверки — партнёрам-антивирусам,[d] так что конфиденциальный документ туда лучше не загружать, а проверка по одной лишь сумме этого недостатка лишена.*(вывод автора)*

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: сумма защищает от подмены по дороге, а не от нечестности источника.

---

[a] Apple: альтернативная дистрибуция приложений на iPhone, на англ. Проверено: 2026-10-11.

[b] DeadHash на GitHub, на англ. Проверено: 2026-10-11.

[c] DeadHash в F-Droid, на англ. Проверено: 2026-10-11.

[d]Документация VirusTotal: как это работает, на англ.; подтверждает передачу содержимого платным клиентам и результатов партнёрам. Проверено: 2026-10-12.

Видео: Tech Talk — Открытый исходный код: гарантирует ли Open Source безопасность данных https://www.youtube.com/watch?v=4UAevts1Qhg

Tech Talk — Открытый исходный код: гарантирует ли Open Source безопасность данных — 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.

Проверить установленные программы

Раз в год открывайте список установленных программ и проходите 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 спросите об одном: пользовались ли вы ею за последний год хоть раз. Нет — удалите. Платная — сначала убедитесь, что у вас есть ключ или аккаунт для повторной установки. Нашли меньше трёх таких программ — удалите сколько есть. Где найти список и как удалить программу — на каждой системе один путь:

Windows: найти и удалить программу

1. «Пуск» ⊠ «Параметры» ⊠ «Приложения» ⊠ «Установленные приложения».[224] Нет такого пункта (старая версия Windows) — откройте Панель управления ⊠ «Программы» ⊠ «Программы и компоненты» и найдите программу там.
2. Найдите нужную программу, выберите «Дополнительно» ⊠ «Удалить».

Типовой сбой: программы нет в списке или удаление не срабатывает — откройте Панель управления ⊠ «Программы» ⊠ «Программы и компоненты» и удалите оттуда.

Официально: Удаление приложений и программ в Windows.

Мас: найти и удалить программу

1. Откройте Finder ⊠ папку «Программы» — это и есть список всех установленных программ.
2. Переключитесь на вид списком и откройте параметры вида Finder («Вид» ⊠ «Показать параметры вида»):[225] отметьте там колонку с датой последнего открытия (в английском интерфейсе — Date Last Opened),*(вывод автора)* по ней видно, что вы не трогали год и больше. Такой колонки нет — вместо неё отсортируйте список по дате изменения.*(вывод автора)*
3. Закройте программу, если она запущена. Если у неё есть собственный деинсталлятор (ищите его в папке программы или в её документации) — воспользуйтесь им: по данным самой Apple, вместе с программой он убирает и её элементы авторизации, расширения и другие связанные данные.
4. Нет деинсталлятора — перетащите программу из «Программы» в корзину, а потом очистите корзину через Finder.

Удаление программы не трогает документы и файлы, которые вы ею создавали, — это отдельно подтверждает сама Apple.

---

[224]Поддержка Microsoft: удаление приложений и программ в Windows; путь «Пуск» ⊠ «Параметры» ⊠ «Приложения» ⊠ «Установленные приложения» ⊠ «Дополнительно» ⊠ «Удалить» и путь через Панель управления. Проверено: 2026-10-13.

[225]Поддержка Apple: параметры вида папки в Finder, на англ.; подтверждает «View > Show View Options» (Command-J). Наличие колонки «Date Last Opened» в списке параметров источник не подтверждает; название встречается в справке Apple только как вариант группировки. Проверено: 2026-10-13.

Официально: Удаление приложений на Mac.

iPhone: найти и удалить приложение

1. «Настройки» ⊠ «Основные» ⊠ «Хранилище iPhone».[226]
2. Откройте нужное приложение в списке и выберите «Удалить приложение»: оно убирает и само приложение, и все его данные.

Официально: Освобождение места в хранилище iPhone.

Android: найти и удалить приложение

1. Google Play ⊠ значок профиля ⊠ «Управление приложениями и устройством» ⊠ «Управление» ⊠ нужное приложение ⊠ «Удалить».
2. Приложение поставлено не из Google Play — «Настройки» ⊠ «Приложения» (на телефонах разных производителей пункты называются по-разному) ⊠ нужное приложение ⊠ «Удалить».*(вывод автора)*

Официально: Удаление приложений.

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. Программа обычно так же легко ставится заново, если вдруг понадобится снова, а совсем старую версию иногда у разработчика уже не найти.

> **Максимум**
>
> **Дополнительно (на выбор).**
>
> *Подсказки, чем вы не пользовались — если не помните.*

[226]Поддержка Apple: проверка хранилища iPhone, на англ.; путь Settings ⊠ General ⊠ iPhone Storage, удаление убирает приложение и его данные. Проверено: 2026-10-13.

- Windows: даты последнего использования в списке «Установленные приложения» нет.
- iPhone: под названием приложения в «Хранилище iPhone» может быть указано, когда его использовали в последний раз; в новых версиях iOS подпись есть не всегда.
- Android: «Цифровое благополучие и родительский контроль» в настройках показывает время использования приложений (доступные показатели зависят от телефона). В Google Play есть и архивирование неиспользуемых приложений: значок остаётся на месте.[a]

«Выгрузить приложение» на iPhone — если нужно освободить место, не теряя данные. Выгрузка освобождает место, но оставляет документы и данные на месте: значок остаётся, а при следующем нажатии приложение ставится заново.[b] Для чистки списка это не подходит.

Разрешения — если хотите проверить глубже, а не только «пользуюсь или нет». 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.

Чек-лист: откройте по очереди «Камера», «Микрофон», «Контакты», «Геолокация» и у приложений, которым этот доступ не нужен, отзовите его. Критерий: не можете назвать, как доступ связан с работой приложения, — выключите.*(вывод автора)*

- Android: «Настройки» ⊠ «Безопасность и конфиденциальность» ⊠ «Конфиденциальность» ⊠ «Управление разрешениями». Список устроен не по программам, а по видам доступа.[c] На телефонах некоторых производителей путь отличается.
- iPhone: «Настройки» ⊠ «Конфиденциальность и безопасность» ⊠ нужный вид доступа (например, «Контакты»

или «Камера») — там список приложений с переключателями;*(вывод автора)* Apple описывает, как управлять доступом к информации в приложениях, в собственной инструкции.

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.

---

[a] Справка Google: удаление приложений, на англ.; описывает архивирование неиспользуемых приложений в Google Play. Проверено: 2026-10-13.

[b] Поддержка Apple: проверка хранилища iPhone, на англ.; выгрузка освобождает место, но оставляет документы и данные. Проверено: 2026-10-13.

[c] Справка Google: управление разрешениями приложений, на англ.; путь Security & Privacy ⊠ Privacy ⊠ Permission manager, разрешения сгруппированы по типам. Проверено: 2026-10-13.

Максимум

Дополнительно (на выбор): песочница. Это инструмент на случай, когда программу всё-таки хочется попробовать, а доверия к ней пока нет вообще никакого. Песочница — 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. Установленное внутри песочницы удаляется при её закрытии и отделено от основной системы. Сеть там по умолчанию включена,[a] абсолютной защиты песочница не даёт.*(вывод автора)*

Windows — если у вас редакция Pro или выше. В Windows такая возможность встроена в систему, в редакциях Pro и выше,[b] называется «Песочница Windows». Включение:

1. Через «Пуск» откройте компоненты системы: поиск «Включение или отключение компонентов Windows»,

галочка Windows Sandbox, подтвердите. Для этого в BIOS должна быть включена виртуализация.
2. При запросе перезагрузите компьютер.
3. После перезагрузки песочница открывается как обычная программа.[c]

Mac — если нужна изолированная копия Windows; по умолчанию UTM. На Mac прямого аналога с той же простотой нет, но есть настоящая замена — виртуальная машина: отдельная, полностью самостоятельная копия системы внутри окна. Основной вариант — UTM: открытый исходный код (лицензия Apache 2.0, часть компонентов под GPL/LGPL),[d] бесплатна при загрузке с сайта; в Mac App Store она платная.[e] Образы ниже рассчитаны на Mac с процессором Apple Silicon.*(вывод автора)* Шаги:

1. Скачайте образ DMG со страницы проекта на GitHub, откройте его и перетащите значок UTM в показанную рядом папку.[f]
2. Скачайте образ Windows 11 для Arm (сборка arm64) со страницы Microsoft; ключ или лицензия на Windows нужны отдельно.[g]*(вывод автора)*
3. В UTM нажмите «+» ⊠ `Virtualize` / `Virtualize` ⊠ `Windows` / `Windows`, выберите объём памяти и число ядер, отметьте `Install Windows 10 or higher` / `Install Windows 10 or higher` и `Install drivers and SPICE tools` / `Install drivers and SPICE tools`, через `Browse` / `Browse` выберите скачанный образ, задайте размер диска, нажмите `Save` / `Save`, затем `Run` / `Run` и следуйте шагам установщика.[h]

По официальным требованиям самой Microsoft, Windows 11 нужно 64 ГБ места на диске, 4 ГБ памяти и два процессорных ядра.[i] Secure Boot и виртуальный TPM 2.0 в новых версиях UTM включаются сами; если установщик Windows их требует, а они выключены, включите в настройках виртуальной машины (раздел QEMU). 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.

Остальные варианты на Mac — если UTM не подошёл:

- VMware Fusion — с 11 ноября 2024 года бесплатна для всех, включая коммерческое использование, но у бесплатных пользователей нет платной поддержки, только документация и сообщество.[j]
- VirtualBox — работает на Mac с Apple Silicon (официальная сборка есть с версии 7.1), но, судя по списку изменений 7.1 (виртуализация Arm для Linux и BSD), рассчитан на гостевые системы для Arm, а не на обычные Windows/Intel-образы.[k]
- Parallels Desktop — платный (в основном по подписке).

---

[a] Microsoft Learn: Песочница Windows, на англ.; подтверждает изоляцию и включённую по умолчанию сеть. Проверено: 2026-10-12.

[b] Microsoft Learn: Песочница Windows, на англ.; подтверждает требование к редакциям (Pro, Enterprise, Education; Home не поддерживается). Проверено: 2026-10-12.

[c] Microsoft Learn: Install Windows Sandbox, на англ. (компонент «Windows Sandbox» в «Turn Windows features on or off», перезагрузка при запросе, виртуализация в BIOS). Проверено: 2026-10-12.

[d] UTM на GitHub, на англ. Проверено: 2026-10-11.

[e] UTM в Mac App Store, на англ. Проверено: 2026-10-11.

[f] Документация UTM: установка на macOS, на англ.; образ DMG с GitHub, значок UTM перетаскивается в показанную рядом папку, версия из App Store идентична. Проверено: 2026-10-13.

[g] Microsoft: загрузка Windows 11 Arm64, на англ.; страница обсуждает только ключ продукта, условия лицензии отдельно не разбирает. Проверено: 2026-10-13.

[h] Документация UTM: Windows, на англ.; шаги мастера создания виртуальной машины с образом arm64; в новых версиях UTM Secure Boot и TPM включаются автоматически, вручную — в настройках QEMU. Проверено: 2026-10-13.

[i] Microsoft Learn: системные требования Windows 11, на англ. Проверено: 2026-10-11.

[j] Блог VMware: Fusion и Workstation теперь бесплатны для всех, на англ. Проверено: 2026-10-11.

[k] VirtualBox: список изменений версии 7.1, на англ.; в списке изменений указана виртуализация Arm для виртуальных машин Linux и BSD. Проверено: 2026-10-12.

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

все такие, если их меньше трёх).

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: это заметно снижает риск, который идёт от установленного софта. *(вывод автора)* 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

Тема для конкретной ситуации: на телефоне есть приложение, которому вы не доверяете, но пользуетесь им, — рабочее приложение с доступом к личной переписке, игра, которая просит контакты непонятно зачем, программа, нужная раз в месяц. Такого приложения нет — остановитесь здесь, это нормально.

Тема подходит, если выполнены оба условия:

1. Есть приложение, которому вы не доверяете.
2. На телефоне нет рабочего профиля от работодателя. Проверка: проведите по экрану снизу вверх. Вкладки «Работа» в списке приложений нет, и в «Настройки» ⊠ «Пароли и аккаунты» вкладки «Работа» тоже нет — профиля нет.[227] Профиль есть — не удаляйте его и остановитесь здесь: Shelter с ним не работает (подробности ниже, в «Если не получилось»).

Сделай это прямо сейчас

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

[227] Рабочий профиль — Справка Google для Android Enterprise. Проверено: 2026-10-13.

Зачем второе пространство на телефоне

Android умеет завести внутри одного телефона второе, полностью отдельное пространство. Приложение внутри него не видит ваши файлы и приложения из основного пространства: у профиля отдельное хранилище и отдельные данные.[228] Исключение — то, что вы сами передаёте через меню «Поделиться» или выбор фото. Если такое приложение подведёт — утечкой, слежкой, жадностью до разрешений, — оно получит в основном то, что вы ему передали, а не всё содержимое телефона. Это перегородка внутри одного устройства, а не отдельный телефон.

Максимум

Дополнительно (на выбор): второй телефон

Выбирайте, если недоверенное приложение вообще не должно жить на одном устройстве с личной перепиской. Второй Android-телефон даёт самое полное разделение: отдельное устройство, отдельные приложения, отдельные данные.

Второй телефон можно использовать по Wi-Fi без SIM: подключите его к точке доступа первого телефона. Коды из SMS на нём получить не получится.

Ограничения: раздача Wi-Fi не защищает первый телефон от его собственной компрометации, точка доступа работает только пока первый аппарат рядом, включён и не разряжен, а второй телефон теряет интернет при её отключении. Это самое полное разделение устройств, но не обещание абсолютной безопасности всей связки.

Поставить F-Droid

F-Droid — открытый каталог программ с открытым исходным кодом, независимый от Google Play. Он ставится не из магазина, а

[228] Private Space — Android Open Source Project, на англ. Проверено: 2026-10-11.

файлом с сайта f-droid.org, и живёт на телефоне рядом с Google Play. Shelter, о которой речь дальше, есть в F-Droid. В Google Play её нет. *(вывод автора)*

Базовый минимум.

1. Откройте в браузере телефона сайт f-droid.org. (☒ установка F-Droid и Shelter).
2. Нажмите `Download F-Droid` / `Download F-Droid`:[229] браузер скачает файл `F-Droid.apk`.
3. Откройте скачанный файл из уведомления о загрузке. *(вывод автора)*
4. Android покажет предупреждение, что установка из этого источника запрещена. Нажмите кнопку перехода в настройки и включите разрешение для браузера, из которого скачали файл.*(вывод автора)* Кнопки нет — откройте «Настройки», введите в строку поиска «Установка неизвестных приложений», выберите свой браузер и включите разрешение.*(вывод автора)*
5. Вернитесь назад кнопкой «Назад», подтвердите установку и откройте F-Droid.

Типовой сбой: предупреждение появляется снова — разрешение включено не тому приложению. Разрешайте то приложение, из которого открыли файл. Если открывали из папки «Загрузки», это приложение «Файлы». *(вывод автора)*

Второй сбой: разрешение включено, а Android всё равно отказывается ставить F-Droid. Скорее всего, действует проверка разработчиков (раздел «Дополнительно» в конце темы). Остановитесь и возьмите встроенное решение — «Частное пространство» или «Защищённую папку» (см. «Дополнительно» в разделе про Shelter).*(вывод автора)*

Получилось — когда F-Droid открывается, а внутри виден список программ.

Проверь себя. Как называется открытый каталог приложений, из

[229] F-Droid, на англ.; кнопка «Download F-Droid» на главной странице ведёт на файл F-Droid.apk. Проверено: 2026-10-13.

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 большинство приложений каталог собирает и подписывает сам по открытому коду (есть исключения с подписью разработчика). Каталог проверяет, что программа собрана из открытого кода, но это не гарантия безопасности. Обратная сторона: приложений там заметно меньше, чем в обычном магазине.

> **Максимум**
>
> **Дополнительно (на выбор).**
>
> *Название пункта разрешения отличается — если на вашем телефоне Samsung, Xiaomi или другая оболочка.* Точный путь в этих оболочках официальной справкой не подтверждён. Используйте поиск по настройкам: «Установка неизвестных приложений» или «Неизвестные источники».*(вывод автора)*
>
> *F-Droid и Google Play — не замена друг другу.* Один не мешает другому. F-Droid — способ ставить программы с открытым кодом в обход магазина Google, а не запасной вариант на случай, когда программы нет больше нигде.

Завести пространство в Shelter

Технически это рабочий профиль — встроенный механизм Android для разделения личного и рабочего. Shelter настраивает его для вас без работодателя.[230] Права суперпользователя и перепрошивка не нужны. *(вывод автора)*

Почему именно Shelter. Правило выбора: сначала открытый исходный код, затем бесплатная, затем самая популярная. Shelter и Insular — открытые и бесплатные оба.[231] Популярность по источ-

[230] Shelter, README (репозиторий на GitHub), на англ. Проверено: 2026-10-13.
[231] Insular на F-Droid, на англ. Проверено: 2026-10-13.

никам я не сравнивал. Решает другое: Insular требует Android 8.1 или новее, по умолчанию зашифрованное устройство и права администратора устройства,[232] а Shelter, судя по описанию проекта, работает на рабочем профиле обычного Android.[233] *(вывод автора)* Поэтому в базе Insular и Island не используются: только Shelter.

Доверие к Shelter стоит на проверяемых вещах: исходный код открыт на GitHub — открытость сама по себе не гарантия, но проверить можно. Последняя версия в F-Droid, 1.9.1, вышла в декабре 2023-го,[234] а сам проект описывает себя как программу в режиме поддержки, а не активной разработки.[235] Это не заброшенность: та же разница между зрелой и мёртвой программой, что и у QuickHash в теме про программы.

Базовый минимум.

Shelter: создание рабочего профиля (проверено в Shelter 1.9.1)

1. Откройте F-Droid, найдите «Shelter» и поставьте Shelter. Android может ещё раз попросить то же разрешение, теперь для самого F-Droid, — включите его тем же путём, что в разделе про F-Droid.
2. Откройте Shelter. Экраны Shelter в версии 1.9.1 английские. Первый экран — предупреждение с кнопками `Continue` / `Continue` и «Bye»: нажмите первую.
3. Дальше идут три вводных экрана: `Welcome to Shelter` / `Welcome to Shelter`, `A word on permissions` / `A word on permissions` и `Compatibility` / `Compatibility`.[236] На каждом прочитайте текст и идите дальше.
4. На экране `Ready?` / `Ready?` идите дальше. Появится `Please wait...` / `Please wait...`: система создаёт рабочий профиль. Ждите до 5 минут*(вывод автора)* и не выключайте экран. (☒ изоляция).
5. Исходов два. Появился `Setup failed` / `Setup failed` — ра-

[232] Insular на F-Droid, на англ. Проверено: 2026-10-13.

[233] Shelter, README (репозиторий на GitHub), на англ. Проверено: 2026-10-13.

[234] Shelter на F-Droid, на англ. Проверено: 2026-10-11.

[235] Shelter, README (репозиторий на GitHub), на англ. Проверено: 2026-10-13.

[236] Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.

бочий профиль уже есть; дальше по этому пути не пройти, см. «Если не получилось». Появился `Action required` / `Action required` — идите к шагу 6.

6. Разверните шторку уведомлений и нажмите `Click here to finish setting up Shelter` / `Click here to finish setting up Shelter`.[237] Дальше идут экраны самой системы Android, не Shelter.
7. Если Android предложит задать отдельный код разблокировки для рабочего профиля — выберите PIN из 6 цифр, не совпадающий с кодом телефона.*(вывод автора)* Графический ключ не выбирайте.*(вывод автора)*
8. Android вернёт вас в Shelter с сообщением `Shelter setup complete. Now restarting Shelter` / `Shelter setup complete. Now restarting Shelter`.[238] Программа перезапустится сама.

Экраны сверены по текстам Shelter, в других сборках могут отличаться.

Официально: исходный код Shelter на GitHub.

Если не получилось.

- `Setup failed` / `Setup failed` — на телефоне уже есть рабочий профиль. Android допускает один рабочий профиль на пользователя.*(вывод автора)* Профиль от работодателя не удаляйте: удалить его можно только если устройство ваше или организация отдала его вам в собственность.[239] Остановитесь на этом: тема вам не подходит.
- Профиль на телефоне когда-то создали вы сами, и устройство ваше — удалите его: «Настройки» ☒ «Пароли и аккаунты» ☒ вкладка «Работа» ☒ «Удалить рабочий профиль» ☒ подтвердите.[240] Данные профиля удаляются. После этого повторите

[237] Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.

[238] Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.

[239] Рабочий профиль — Справка Google для Android Enterprise. Проверено: 2026-10-13.

[240] Рабочий профиль — Справка Google для Android Enterprise. Проверено: 2026-10-13.

шаги с 2-го.
- Xiaomi с MIUI: по строкам самой Shelter, клонирование стороннего приложения на MIUI невозможно (обход — клонировать магазин приложений);[241] на HyperOS не проверялось. Возьмите «Клонирование приложений» из раздела «Дополнительно» ниже.

Получилось — когда в Shelter открываются две вкладки: «Main» и «Shelter».[242]

Видео: Tech Talk — Как изолировать приложения на Android с Shelter: Полная защита данных (2025) https://www.youtube.com/watch?v=DX8QAqKDi8Y

Tech Talk — Как изолировать приложения на Android с Shelter: Полная защита данных (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**
>
> **Дополнительно (на выбор).**
>
> *Встроенное решение вместо Shelter — когда его брать.* Берите встроенное, если на телефоне уже есть нужный пункт и вы не хотите ставить сторонние приложения. Порядок выбора: Android 15 или новее и нет рабочего профиля — «Частное пространство»; Samsung — «Защищённая папка»; Xiaomi — «Клонирование приложений»; иначе — Shelter из базы.
>
> *Частное пространство (Private Space) — Android 15 и новее.*

[241] Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.

[242] Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.

Путь: «Настройки» ⊠ «Защита и конфиденциальность» ⊠ в разделе «Конфиденциальность» пункт «Частное пространство».[a] У других производителей название и путь могут отличаться. Дальше следуйте шагам на экране и задайте отдельную блокировку пространства.[b] Приложение ставится изнутри пространства кнопкой «Установить» или долгим нажатием на значок приложения в списке ⊠ «Установить приложение в частное пространство»; данные из личной копии не переносятся.[cd] Google-аккаунт для пространства не обязателен; если входите, используйте отдельный аккаунт, нигде больше не использованный, — иначе синхронизированные фото, история браузера и пароли могут стать доступны вне пространства.[e] Заблокированное пространство полностью останавливает свои приложения: те, которым нужна фоновая работа, внутри не подойдут; их трафик идёт мимо VPN устройства.[f] Недоступно на управляемых организацией устройствах.[g]

Защищённая папка (Secure Folder) — Samsung. Настройки ⊠ Защита и конфиденциальность ⊠ Другие настройки безопасности ⊠ Защищённая папка (в английском интерфейсе Settings > Security and privacy > More security settings > Secure Folder; на других версиях One UI и в русском интерфейсе подписи могут отличаться — ищите «Защищённая папка» через поиск по настройкам). Для неё обязателен аккаунт Samsung.[h]

Клонирование приложений (Dual apps) — Xiaomi. Настройки ⊠ Приложения ⊠ Клонирование приложений. Путь и название зависят от версии прошивки и официальной справкой не подтверждены. Пункт «Второе пространство» на Xiaomi — другой механизм, для переноса одного приложения он не нужен.*(вывод автора)*

Island и Insular — только если Shelter вам не подошла. Island в F-Droid нет: там лежит Insular, форк Island без компонентов Google. Он по умолчанию требует Android 8.1 или новее и зашифрованное устройство; удалять его нужно через «Destroy Insular» в настройках приложения, иначе рабочий профиль

останется.[i]

[a]Частное пространство — Справка Google. Проверено: 2026-10-13.
[b]Private space — Справка Google, на англ. Проверено: 2026-10-13.
[c]Частное пространство — Справка Google. Проверено: 2026-10-13.
[d]Private space — Справка Google, на англ. Проверено: 2026-10-13.
[e]Частное пространство — Справка Google. Проверено: 2026-10-13.
[f]Private space — Справка Google, на англ. Проверено: 2026-10-13.
[g]Private space — Справка Google, на англ. Проверено: 2026-10-13.
[h]Samsung, Secure Folder, на англ. Проверено: 2026-10-11.
[i]Insular на F-Droid, на англ. Проверено: 2026-10-13.

Перенести приложения во второй профиль

Что переносить. Берите то приложение, которое просит больше всего разрешений (контакты, микрофон, геолокация) при простой функции: сканер документов, конвертер файлов, простой редактор фото. Такого нет — не переносите ничего: тема вам не нужна. Банковские и платёжные приложения не переносите: они могут не заработать в рабочем профиле.*(вывод автора)*

Базовый минимум.

1. Откройте Shelter, вкладка «Main». Нажмите на название нужного приложения в списке и выберите в окне пункт `Clone to Shelter (Work Profile)` / `Clone to Shelter (Work Profile)`.[243] (⊠ клонирование приложения). В первый раз Shelter может попросить разрешение на установку — включите его тем же путём, что и для F-Droid, только для Shelter.*(вывод автора)*
2. Дождитесь сообщения «Application “название” cloned successfully».[244]
3. Откройте клон: проведите по экрану снизу вверх и откройте вкладку «Работа»; рабочие приложения помечены значком портфеля.[245] Если вкладки «Работа» нет, ищите значок с порт-

[243]Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.
[244]Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.
[245]Рабочий профиль — Справка Google для Android Enterprise. Проверено: 2026-

фелем среди остальных.*(вывод автора)* Войдите в аккаунт заново: клон — пустая установка, данных личной копии в нём нет.*(вывод автора)*

4. Сделайте в клоне то, ради чего приложение нужно. Получилось — удалите оригинал из личного профиля: Google Play ☒ значок профиля ☒ «Управление приложениями и устройством» ☒ «Управление» ☒ приложение ☒ «Удалить».[246] Проверьте, что значок клона в разделе «Работа» остался на месте.*(вывод автора)* Не получилось — пользуйтесь оригиналом, клон не нужен.

Типовой сбой: окно показывает «Cannot clone system apps to a profile that Shelter has no control of.» — системные приложения не клонируются.[247] Выберите другое приложение.

Получилось — когда у приложения две иконки: личная и рабочая (с портфелем), а оригинал удалён.

Максимум

Дополнительно (на выбор).

Рабочее и личное — если нужно просто разнести их по разным углам. Выбирайте, когда вопрос не в недоверии, а в удобстве. Рабочую почту, корпоративный мессенджер и таск-трекер можно держать в отдельном профиле и вечером ставить профиль на паузу (см. следующий раздел) — вместо того чтобы полагаться на силу воли не открывать почту. Личный профиль выигрывает тоже: рабочие иконки, звуки и бейджи не мешаются среди личных весь день.

Приложение от работодателя. У него своя политика безопасности и свои требования к устройству. Если оно ставится политикой работодателя через рабочий профиль, Shelter на этом

10-13.

[246] Справка Google: удаление приложений; описан путь только через Google Play. Проверено: 2026-10-13.

[247] Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.

телефоне не заработает (см. «Если не получилось»).

Пользоваться вторым пространством

Иконки рабочих копий выглядят как обычные, но помечены значком портфеля, а на части лаунчеров, в том числе на чистом Android, собраны на вкладке «Работа» в списке приложений.[248] Открываются они одним касанием.

Базовый минимум: пауза всего профиля.

1. Проведите по экрану снизу вверх и откройте вкладку «Работа».[249]
2. Переключите внизу экрана `Pause work apps` / `Отключить рабочие приложения` в положение «ВЫКЛ»: профиль на паузе. Приложения профиля не запускаются, не показывают уведомления и не тратят батарею.[250]
3. Чтобы вернуть профиль, включите тот же переключатель. Проверьте, что переключатель снова включён и вкладка «Работа» открывается.[251]

(☒ настройки рабочего профиля).

Сделайте паузу один раз на пробу — просто чтобы знать, как это работает.

Типовой сбой: уведомления клона не приходят — профиль на паузе. Включите переключатель обратно.[252] Если вкладки «Работа» в вашем лаунчере нет, на панели быстрых настроек есть карточка рабочего профиля: затемнена — профиль на паузе.[253]

[248]Рабочий профиль — Справка Google для Android Enterprise. Проверено: 2026-10-13.
[249]Приостановка рабочего профиля — Справка Google. Проверено: 2026-10-13.
[250]Приостановка рабочего профиля — Справка Google. Проверено: 2026-10-13.
[251]Приостановка рабочего профиля — Справка Google. Проверено: 2026-10-13.
[252]Приостановка рабочего профиля — Справка Google. Проверено: 2026-10-13.
[253]Приостановка рабочего профиля — Справка Google. Проверено: 2026-10-13.

Максимум

Дополнительно (на выбор): заморозка одного приложения.

Выбирайте, если приложение нужно редко — раз в месяц и реже. Заморозка действует на одну программу, а не на весь профиль: замороженное приложение не запускается, пока вы его не разморозите.[a]

1. Откройте Shelter, вкладка «Shelter».[b]
2. Нажмите на название приложения и выберите `Freeze` / `Freeze`. Появится сообщение «Application “название” frozen successfully».[c]
3. Когда понадобится — тем же путём выберите `Unfreeze` / `Unfreeze` или `Unfreeze and Launch` / `Unfreeze and Launch`.[d]

В настройках Shelter есть `Auto Freeze Service` / `Auto Freeze Service`: при блокировке экрана он замораживает приложения, запущенные через ярлык «Unfreeze & Launch».[e] Экраны сверены по текстам Shelter, в других сборках могут отличаться.

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

---

[a] Shelter, README (репозиторий на GitHub), на англ. Проверено: 2026-10-13.

[b] Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.

[c] Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.

[d] Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.

[e] Shelter, строки интерфейса (strings.xml в репозитории на GitHub), на англ. Проверено: 2026-10-13.

Какие у второго пространства ограничения

Изоляция не абсолютная: это плотная перегородка, а не бетонная стена. Правила, которые экономят время:

1. Банковские и платёжные приложения в профиль не переносите. Остальные сначала проверьте в клоне и только потом удаляйте оригинал.*(вывод автора)*
2. Клон — свежая пустая установка: войти придётся заново, данных личной копии он не видит. В этом смысл разделения и его цена.*(вывод автора)*
3. Раз в месяц*(вывод автора)* открывайте F-Droid и обновляйте Shelter. Как обновляются клоны, источники не говорят — Shelter следить за версиями не обещает, поэтому проверяйте версию клона сами.*(вывод автора)*
4. Удаление профиля необратимо: корзины и отмены нет, все приложения и данные профиля пропадают.[254] Сначала заберите из клонов нужное. Затем: «Настройки» ⊠ «Пароли и аккаунты» ⊠ вкладка «Работа» ⊠ «Удалить рабочий профиль» ⊠ подтвердите.[255] Только после этого удалите саму Shelter.[256]
5. Первое время путают значки двух копий одного мессенджера и вопрос системы, каким профилем открыть ссылку. Привычка приходит не сразу, это нормально.*(вывод автора)*

> **Максимум**
>
> **Дополнительно (на выбор): проверка разработчиков Google.**
>
> *Читайте, если ставите программы вне Google Play.* Есть оговорка про сам путь установки, которым на телефон попадают и F-Droid, и Shelter. Google требует, чтобы приложения на сертифицированных Android-устройствах приходили от раз-

[254] Рабочий профиль — Справка Google для Android Enterprise. Проверено: 2026-10-13.

[255] Рабочий профиль — Справка Google для Android Enterprise. Проверено: 2026-10-13.

[256] Shelter, README (репозиторий на GitHub), на англ. Проверено: 2026-10-13.

работчика с подтверждённой личностью — в первую очередь для магазинов-участников; установка вне магазина остаётся возможной через adb или «расширенный» путь. Регистрация разработчиков началась в марте 2026-го, а с 30 сентября 2026-го правило действует в Бразилии, Индонезии, Сингапуре и Таиланде. Google планирует расширить требование на весь мир в 2027 году и позже.[a] Для тех, кто всё же захочет поставить неподтверждённое приложение, предусмотрен нарочито неудобный обходной путь — включить режим разработчика, подождать 24 часа и несколько раз согласиться с предупреждениями; с августа 2026-го Google начала постепенно включать этот путь.[b] Есть и бесплатная регистрация «для ограниченного распространения», но она рассчитана всего на 20 устройств.[c] Сам F-Droid ещё в феврале 2026-го публично выступил против этих правил, назвав их угрозой для себя: для его каталога обязательная регистрация разработчиков и ID у Google создаёт угрозу.[d]

Что это значит для вас: вне Бразилии, Индонезии, Сингапура и Таиланда правило по состоянию на 13 октября 2026-го пока не применяется; в этих странах оно действует с 30 сентября 2026-го. 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.

[a] Android Developers Blog, проверка разработчиков, на англ. Проверено: 2026-10-12.

[b] 9to5Google, пересказ в новостной статье, на англ. Проверено: 2026-10-12.

[c] Android Developers Blog, проверка разработчиков, на англ. Проверено: 2026-10-12.

[d] F-Droid, открытое письмо против проверки разработчиков, на англ. Проверено: 2026-10-11.

Итог: второе пространство окупает потраченное время только при одном условии — на телефоне завелось приложение, которому не хочется доверять остальной телефон целиком. Нет такого приложения — тема не понадобится, без драмы. Девять тем про риск на этом заканчиваются — обязательная часть позади. Дальше одна те-

ма вне очереди, «Основы работы с нейросетями»: она про то, как кое-чему научиться, а не про то, как ничего не потерять, — относитесь к ней 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 DeepSeek и задать ему вопрос без личных данных — 5 минут
- ☐ Переспросить то же самое одной готовой фразой: списком из 5–7 шагов — 3 минуты
- ☐ Проверить в ответе один факт, на основании которого вы будете действовать — 5 минут

Что такое чат-бот

Проще всего представить его не поисковиком со справочником, а очень начитанным приятелем, который предсказывает продолжение текста. Он строит ответ на закономерностях, усвоенных из огромного количества текстов, а не сверяется со списком фактов. Правда, некоторые сервисы умеют и искать в интернете (см. ниже), и тогда часть ответа опирается на найденные страницы.[257] (☒ как модель угадывает следующее слово).

[257] OpenAI Help: Does ChatGPT tell the truth? и Claude Help: Enabling and using web search (поиск в интернете есть минимум у двух сервисов), на англ. Проверено: 2026-10-12.

Отсюда прямое и не самое удобное следствие: такой приятель умеет **уверенно ошибаться**. Пользователю он не показывает, насколько уверен в каждом факте: модели способны оценивать собственную уверенность в ответе,[258] но в тексте ответа эта оценка не видна, и по тону её не прочитать. Точный факт и чистая выдумка рождаются одним и тем же способом, поэтому и звучат одинаково гладко. По одному тону ответа отличить одно от другого попросту нельзя.[259] (⊠ почему ошибки неизбежны).

Видео: Тостер Скрипт — Почему нейросети постоянно врут? (и почему этого уже не исправить) https://www.youtube.com/watch?v=Ip2_wpHLv-k

Тостер Скрипт — Почему нейросети постоянно врут? (и почему этого уже не исправить) — подсказка к тому, как чат-бот строит ответ и почему выдумывает; ролик разговорный, с примерами на небольшой модели, которую автор запустил у себя.

- 2:24 — как нейросеть угадывает следующее слово
- 5:58 — все ответы выдумка, галлюцинации не исправить
- 8:10 — убедительная выдумка про несуществующий кроссовер

Попробовать чат-бот в сервисе

Сервисов три: DeepSeek, ChatGPT и Grok. Вы берёте один, по порядку: сначала тот, у которого открыт исходный код, потом бесплатный, потом самый популярный. Первый по этому порядку — DeepSeek: он публикует веса своих моделей под лицензией MIT.[260] Открыты именно веса моделей, а не сам чат на сайте: чат остаётся сервисом компании. ChatGPT — запасной сервис на случай, если DeepSeek не открылся.

Базовый минимум.

[258] Kadavath et al., Language Models (Mostly) Know What They Know (arXiv:2207.05221), на англ. Проверено: 2026-10-12.

[259] OpenAI Help: Does ChatGPT tell the truth?, на англ. Проверено: 2026-10-11.

[260] DeepSeek-V4.1-Flash на Hugging Face (карточка модели), «This repository and the model weights are licensed under the MIT License», на англ. Проверено: 2026-10-13.

1. Откройте chat.deepseek.com. Если открылась главная страница deepseek.com, нажмите на ней «Chat with DeepSeek».[261]
2. Зарегистрируйтесь по электронной почте, заведя для этого отдельный ящик у любого почтового сервиса: основной ящик для таких регистраций не используйте.*(вывод автора)* Адрес почты DeepSeek называет среди данных аккаунта.[262] Идите по подсказкам на экране.
3. Задайте первый вопрос: реальный, но без личных данных. Например: `Объясни простыми словами, что значит «неустойка» в договоре аренды. Ответ — до десяти строк.` Вопрос пишется в поле для сообщения на странице чата.
4. Не отправляйте в чат-бот пароли, паспортные данные, медицинские и финансовые документы, рабочие документы и чужие переписки. Всё отправленное уходит в чужую компанию: DeepSeek хранит данные пользователей в КНР, использует запросы для обучения своих моделей, а отказ от этого — через письмо на privacy@deepseek.com.[263] Подробности и чистка уже отправленного — в теме про безопасность при использовании ИИ, раздел «Убрать лишнее из запроса чат-боту».
5. Не открылась страница или регистрация не прошла с первой попытки — не тратьте время и откройте chatgpt.com. В странах, где ChatGPT поддерживается, он открывается без аккаунта, и переписка у вас не сохраняется: закрыли браузер — разговора нет.[264] Не открылся и он — вернитесь к DeepSeek позже или сделайте остальные практики темы на любом доступном сервисе: цикл «спросил — прочитал — переспросил» везде одинаковый.

Получилось — когда в одном из сервисов открыт диалог, а в нём

[261]DeepSeek: главная страница, кнопка «Chat with DeepSeek»; бесплатность чата страница не называет, на англ. Проверено: 2026-10-13.

[262]DeepSeek Privacy Policy, в данных аккаунта названы адрес почты и телефон; названия кнопок регистрации политика не приводит, на англ. Проверено: 2026-10-13.

[263]DeepSeek Privacy Policy, данные хранятся в КНР, запросы используются для обучения моделей, отказ от этого — письмом на privacy@deepseek.com, историю чата можно удалить в настройках; точный путь в меню политика не приводит, на англ. Проверено: 2026-10-13.

[264]OpenAI Help: The ChatGPT home page, на англ. Проверено: 2026-10-11.

лежит ответ на ваш реальный вопрос без личных данных.

Максимум

Дополнительно (на выбор): регистрация в других сервисах. Берите, если не хотите заводить отдельный ящик под DeepSeek или он вам не открывается. ChatGPT в поддерживаемых странах пускает без аккаунта (шаг 5 выше). В Grok официальная справка xAI называет вход через аккаунт X и позволяет добавить другие способы входа на accounts.x.ai.[a] Какие ещё способы входа есть у Grok и у DeepSeek, кроме перечисленных, официальные источники не подтверждают.

[a] xAI Docs: Accounts FAQ, регистрация через аккаунт X и добавление других способов входа на accounts.x.ai; почта, Google и Apple на этой странице не названы, на англ. Проверено: 2026-10-13.

Задать вопрос боту

Хороший запрос состоит из четырёх частей: задача, ситуация, формат, объём. (☒ как формулировка влияет на ответ). Модель не знает вашей ситуации и достраивает недостающее наиболее вероятным образом, а не по тому, что вы на самом деле имели в виду. Чем меньше вы оставили на догадки, тем меньше придётся переделывать. (☒ почему модели нужно объяснять очевидное).

Базовый минимум.

1. Напишите запрос по шаблону, подставив своё вместо слов в скобках: `Задача: (что нужно сделать). Ситуация: (что случилось и что уже пробовали). Формат: (письмо, список, таблица). Объём: (до скольких строк).`
2. Прочитайте ответ. Не устроил — не начинайте разговор заново. Отправьте второй фразой ровно эти слова: `Перепиши списком из 5–7 шагов простыми словами.` Диалог тот же, вопрос тот же, ответ приходит в нужном виде.*(вывод автора)*
3. Типовой сбой: ответ ушёл не туда по смыслу, а не по виду. То-

гда скажите, что не так и каким ответ должен быть: `Ты поня л неверно: мне нужно (что именно).`

Первый ответ нередко приходится уточнять, потому что вопрос был общим и достраивать пришлось слишком многое.*(вывод автора)* Это нормальный ход работы, а не сбой и не повод считать себя неспособным разобраться: весь навык в переспрашивании.

Получилось — когда вы переспросили тот же вопрос фразой из шага 2 и ответ на глазах стал списком из 5–7 шагов.

Видео: RationalAnswer — Как работает ChatGPT: объясняем нейросети просто https://www.youtube.com/watch?v=VVfFf_XW8zw

RationalAnswer — Как работает ChatGPT: объясняем нейросети просто — подсказка только к тому, почему результат зависит от формулировки запроса; остальной ролик (39 минут, 2023 год) про устройство моделей, смотреть целиком не нужно.

- 26:13 — промпты: от формулировки зависит качество ответа
- 28:11 — модели нужно объяснять то, что людям очевидно

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.

> **Максимум**
>
> **Дополнительно (на выбор): готовые фразы для сложной задачи.** Берите, когда простого запроса по шаблону уже мало.
>
> - Роль: `Побудь редактором этого письма: исправь ошибки, смысл не меняй.` Берите, когда важен тон ответа.*(вывод автора)*
> - Пример: `Вот пример нужного результата: (вставьте пример).` Берите, когда формат необычный и словами его описывать долго.*(вывод автора)*
> - Рассуждение: `Рассуждай по шагам.` Берите, когда в задаче несколько действий подряд. Пошаговый вывод удобно проверять, но верность рассуждения он не гарантирует.*(вывод автора)*
>
> Главное для любой фразы — доводить ответ итерациями, а не соглашаться с первым черновиком: это то же переспрашивание из базового шага 2.

Что умеют бесплатные версии

Базовый минимум. Для первого вопроса платный тариф не нужен: берите бесплатную версию того сервиса, который открылся.*(вывод автора)* Бесплатной версии обычно хватает, чтобы набросать и вычитать текст, объяснить что-то простыми словами, перевести, пересказать длинный текст коротко.*(вывод автора)* Упёрлись в лимит — подождите, пока он сбросится, или продолжите в запасном сервисе (шаг 5 раздела «Попробовать чат-бот в сервисе»). Платить ради этого не нужно.

> **Максимум**
>
> **Дополнительно (на выбор): чем сервисы отличаются.** Бе-

рите, чтобы выбрать сервис под свою задачу, а не по умолчанию.

- ChatGPT: берите, если нужны поиск по интернету, картинки или голосовой режим. Они есть уже в бесплатной версии, но картинки и голос с ограничениями.[a] Лимиты касаются в основном картинок, файлов и голоса, текстовые чаты почти не ограничены.[b]
- Grok: берите, если нужны картинки или видео, но они создаются только на платном тарифе (SuperGrok); в бесплатной версии этого нет.[c]
- DeepSeek: берите, если важны открытые веса моделей. Что чат бесплатный, официальные источники прямо не подтверждают; на сайте компании цены есть только у API.*(вывод автора)*

Цифр лимитов бесплатных тарифов здесь нет: компании меняют их без предупреждения, а на страницах тарифов они обычно описаны словами. Актуальное смотрите на страницах openai.com/chatgpt/pricing и x.ai/pricing. Попробовать один и тот же вопрос в разных сервисах — законный способ понять, какой удобнее лично вам.

---

[a] OpenAI: тарифы ChatGPT, на англ. Проверено: 2026-10-11.

[b] OpenAI Help: Using ChatGPT's free tier FAQ, на англ. Проверено: 2026-10-12.

[c] xAI: тарифы Grok, на англ. Проверено: 2026-10-11.

Максимум

Дополнительно (на выбор): временный чат в ChatGPT. Берите, если вошли в ChatGPT с аккаунтом и хотите спросить о личном. Режим Temporary Chat не попадает в историю, не создаёт «память» и не используется для обучения моделей, но OpenAI может хранить его копию до 30 дней для безопасности.[a] Русская подпись режима в интерфейсе официальной справкой не подтверждена: ищите в чате пункт Temporary Chat. Для вопросов о паспорте, документах и паролях это всё

равно не выход: такое в чат-бот не отправляют (шаг 4 раздела «Попробовать чат-бот в сервисе»).

[a] OpenAI Help: Temporary chat in ChatGPT, страница при проверке не открылась напрямую, сведения взяты из её пересказа в выдаче поиска; русская подпись режима не подтверждена, на англ. Проверено: 2026-10-13.

Проверить ответы бота

Модель способна на уверенные выдумки: заявляет несуществующий факт или источник тем же ровным уверенным тоном, что и правду. Для этого явления есть отдельное слово, «галлюцинации», и означает оно именно это: ответ звучит убедительно, а проверки не выдерживает.[265] (☒ пример убедительной выдумки). Поэтому факт, от которого зависят ваши действия, проверяют отдельно.

Базовый минимум.

1. Выберите в ответе один факт — тот, на основании которого вы будете действовать: срок, сумма, дозировка, адрес. Остальное можно не проверять.
2. Вбейте этот факт в обычный поисковик и найдите два независимых источника, которые сходятся.*(вывод автора)* Два пересказа одной новости — это один источник, а не два.
3. Факт официальный — срок, тариф, норма закона — идите сразу к первоисточнику: на сайт самого ведомства или в текст закона, а не к тому, кто его цитирует.
4. Вопрос про недавние события проверяйте так же обязательно: модель могла о них не знать или найти не то.*(вывод автора)*
5. Типовой сбой: двух сходящихся источников нет или они расходятся. Тогда считайте факт непроверенным и не действуйте на его основании.*(вывод автора)*

На один факт уйдёт около 5 минут.*(вывод автора)*

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

[265] OpenAI Help: Does ChatGPT tell the truth?, на англ. Проверено: 2026-10-11.

ным.

Максимум

Дополнительно (на выбор): сверка со вторым сервисом. Берите, когда факт неофициальный и нужна быстрая проверка до поиска. Задайте тот же вопрос второму сервису, например ChatGPT без аккаунта. Разошлись ответы — точно проверяйте по первоисточнику. Сошлись — доверия больше, но это ещё не доказательство. На это уйдёт около 3 минут.*(вывод автора)*

- ☐ 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 склонен уверенно отвечать там, где честнее было бы сказать «не знаю», — спрашивать у него полезно, а вот верить на слово в вопросах денег и здоровья не стоит. Первый ответ нередко приходится уточнять: чаще всего просто потому, что вопрос был общим. Переспросить тут не признание неудачи, а рабочий способ довести ответ до нужного вида.

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 пароль из переписки и сменить его — 3 минуты
- ☐ Перенести в базу первый из пяти важных сайтов (банк) — 5 минут
- ☐ В мастере создания базы поставить время расшифровки на 3 секунды; вкладку `Advanced` 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 2FAS и включить резервную копию — 8 минут
- ☐ 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 месяц — 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.
☐ Входить в банк из закладки или из приложения банка, а в почту — из закладки — 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 значок слева от адреса (замок или значок настроек) ☒ «Подключение защищено» ☒ «Действительный сертификат» 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
- ☐ Поставить VPN и подключиться — 5 минут
- ☐ Завести отдельный почтовый адрес под регистрации в магазинах и рассылки.
- ☐ Создать аккаунт в 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 — 5 минут
- ☐ Перенести в рабочий профиль одно приложение, которому не доверяете — 5 минут
- ☐ Заморозить в рабочем профиле приложение, которое нужно раз в месяц.
- ☐ Открыть DeepSeek и задать ему вопрос без личных данных — 5 минут
- ☐ Переспросить то же самое одной готовой фразой: списком из 5–7 шагов — 3 минуты
- ☐ Проверить в ответе один факт, на основании которого вы будете действовать — 5 минут
- ☐ Задать один и тот же важный вопрос двум сервисам из трёх и сравнить ответы.