

Руководство по жизни с высокой отдачей (高性价比人生指南). Неофициальный русский перевод книги «高性价比人生指南». Автор русской версии: Максим Ланиес, max0r@yandex.ru. Текст: CC BY 4.0. Сайт: <https://howtolivebetter.ru/>. Версия от 13.10.2026.

14. Безопасность аккаунтов и информации

Рамки: деньги и личная информация. Если кто-то войдёт в ваш аккаунт, первыми вы потеряете деньги. Этот человек также будет использовать ваш аккаунт, чтобы обманывать людей из вашего списка контактов. Это всё равно что кто-то присвоил вашу личность.

1. Включите двухэтапную проверку для почты, платёжных и социальных аккаунтов: в первую очередь выбирайте подтверждение во всплывающем окне на телефоне, и лишь затем — код из СМС

- Выгодность исходной версии: очень высокая
- Доказательность A · исходная версия
- для денег
- бесплатно
- мимоходом
- без силы воли
- Не зависит от страны

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Двухэтапная проверка означает, что при входе, помимо пароля, нужно ещё раз подтвердить, что это действительно вы. Если на телефоне всплывает окно, а вы нажимаете кнопку подтверждения, это блокирует более 90% попыток кражи аккаунта через фишинг. Старые способы с ответами на вопросы «Откуда вы входили в прошлый раз?» или «Какой у вас резервный адрес электронной почты?» блокируют лишь около 10% таких попыток.

Затраты

Бесплатно. Настроить нужно один раз для каждого аккаунта, это займёт две-три минуты.

Выгода

Google проанализировал 350 тыс. реальных попыток кражи аккаунтов, также называемой захватом аккаунтов. Один вид проверки — с помощью устройства: например, на телефоне всплывает окно, в котором нужно нажать кнопку подтверждения, или нужно подключить аппаратный ключ безопасности. Этот вид проверки заблокировал «более 94% попыток захвата аккаунтов через фишинг и 100% автоматизированных попыток захвата». Фишинг — это когда вас обманом заставляют ввести пароль на поддельном сайте. Автоматизированные попытки — это когда программа массово пробует войти с утёртыми паролями. Другой вид проверки — с помощью ответов на вопросы: например, откуда вы входили в прошлый раз или какой у вас

резервный адрес электронной почты. Этот вид проверки «блокировал вплоть до всего 10% попыток захвата через фишинг и 73% автоматизированных попыток захвата»

Примечания

То же исследование показало, что такая проверка иногда не пускает в аккаунт и самого владельца. 52% настоящих пользователей не смогли войти с первой попытки, но в итоге 97% всё же вошли. Сначала включите эту функцию для почты, потому что пароль от большинства других аккаунтов можно восстановить через почту. Используйте коды подтверждения только сами. Какие последствия могут быть, если сообщать коды или проходить проверку по лицу за других, см. в разделе 8, пункте [45](#) (зачитывание кода подтверждения)

Источники

Источники исходной версии

1. Doerfler P, Thomas K, Marincenko M, et al. (2019). Evaluating Login Challenges as a Defense Against Account Takeover. The World Wide Web Conference (WWW '19). doi.org/10.1145/3308558.3313481

[Предложить правку](#) — ошибка, устаревший закон или лучший источник.

2. Отдельный пароль для почты, который не повторяется ни на одном сайте

- Выгодность исходной версии: высокая
- Доказательность С · исходная версия
- для денег
- бесплатно
- мимоходом
- немного силы воли
- Частично Китай
- Российские данные: частично

Китайские условия и российские данные разделены по полям. Российская сверка частичная; непроверенные поля отмечены отдельно. Оценки и фильтры относятся к исходной версии.

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Китай — исходная версия. Пароль, украденный на другом сайте, могут использовать, чтобы сразу войти в вашу почту. Если кто-то войдёт в вашу почту, вы потеряете вместе с ней все аккаунты, пароли к которым можно восстановить через неё. Поэтому пароль для почты должен быть отдельным и нигде больше не использоваться.

Россия. В России так же предлагают защищать учётные записи от мошенников и помогают восстановить контроль над ними. Но в выдержках речь идёт о Госуслугах, а не о почте: дополнительной защитой может стать доверенный контакт. При восстановлении пароля ему приходит СМС, и он подтверждает запрос, только убедившись, что пользователя не обманывают.

Затраты

Китай — исходная версия. Бесплатно. Если хранить пароль в менеджере паролей, не нужно запоминать его самостоятельно. Сложнее всего отказаться от старой привычки использовать один пароль везде.

Россия. Стоимость в этих источниках не указана.

Выгода

Китай — исходная версия. Когда утёкшие с других сайтов логины и пароли по очереди пробуют использовать для входа, это называется подстановкой украденных учётных данных. Это самый простой способ атаки, и в вашу почту тоже будут пытаться войти таким образом. Если кто-то войдёт в вашу почту, вы потеряете все аккаунты, пароли к которым восстанавливаются через неё. Агентство по кибербезопасности и безопасности инфраструктуры США (美国网络安全和基础设施安全局) рекомендует: для каждого аккаунта использовать свой надёжный пароль длиной не менее 16 символов и хранить его в менеджере паролей

Россия. Доверенный контакт даёт дополнительную защиту учётной записи на Госуслугах от мошенников.

Примечания

Китай — исходная версия. Если не можете запомнить пароли, используйте встроенный менеджер паролей браузера. Он запоминает за вас пароль для каждого сайта. Это гораздо лучше, чем использовать один и тот же пароль везде. Не храните пароли в разделе «Избранное» приложения WeChat (微信) или в заметках

Россия. Требований к отдельному паролю для почты, его длине, повторному использованию и хранению в менеджере паролей в этих источниках нет.

Источники

Китай — исходная версия — источники

1. US CISA. Use Strong Passwords. www.cisa.gov/secure-our-world/use-strong-passwords

Россия — источники

1. Безопасность. Проверено 08.10.2026. med-b-kgbuz-rybinskaya-rb-zaozyornyj-r04.gosweb.gosuslugi.ru/inform...

[Предложить правку](#) — ошибка, устаревший закон или лучший источник.

3. Установите пароль блокировки экрана телефона и PIN-код SIM-карты, чтобы защитить аккаунты при потере телефона

- Выгодность исходной версии: очень высокая
- Доказательность С · исходная версия

- для денег
- бесплатно
- мимоходом
- без силы воли
- Не зависит от страны

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

SIM-карта — это маленькая карточка внутри телефона. Через неё приходят SMS с кодами подтверждения. Если телефон потеряется, нашедший его человек может вынуть эту карту, вставить в другой телефон, получать коды подтверждения и по очереди сбрасывать пароли от ваших аккаунтов. Установите PIN-код для карты. Если её переставят в другой телефон, при включении сначала потребуется ввести этот код. Этот путь будет закрыт.

Затраты

Бесплатно. Пароль блокировки экрана и PIN-код достаточно установить по одному разу.

Выгода

После потери телефона самый быстрый путь для нашедшего его человека — вставить SIM-карту в другой телефон и получать ваши SMS с кодами подтверждения. С этими кодами он сможет один за другим сбрасывать пароли от ваших аккаунтов. Если для SIM-карты установлен PIN-код, после перестановки в другой телефон при включении сначала потребуется ввести пароль. Нашедший телефон человек не сможет получать через неё коды подтверждения

Примечания

PIN-код задаётся в пункте «Блокировка SIM-карты» в настройках телефона. Заводской код обычно 1234 или 0000. Если три раза подряд ввести неверный код, разблокировать карту можно будет только с помощью PUK-кода, выданного оператором. Поэтому после установки кода сразу запишите его на бумаге

Источники

Источники исходной версии

1. 作者经验，无直接文献

[Предложить правку](#) — ошибка, устаревший закон или лучший источник.

4. Если потеряли телефон, действуйте в таком порядке: заблокируйте SIM-карту как утраченную, удалённо

заблокируйте телефон, смените пароли, заявите в китайскую полицию, заморозьте банковские карты

- Выгодность исходной версии: очень высокая
- Доказательность С · исходная версия
- для денег
- бесплатно
- мимоходом
- без силы воли
- Частично Китай
- Аналог в России не найден

Искали в официальных российских источниках (проверено 08.10.2026), прямого аналога не нашли. Это не значит, что его нет. Китайские условия на Россию не переносите.

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Китай — исходная версия. Порядок действий важнее быстроты рук. Первым делом заблокируйте SIM-карту как утраченную — так вы перекроете важнейший канал получения кодов подтверждения. Затем удалённо заблокируйте телефон, с компьютера смените пароли от электронной почты и платёжных сервисов, после этого заявите в китайскую полицию и получите подтверждение приёма заявления. В конце, в зависимости от ситуации, заморозьте банковские карты. Если телефона нет при вас, можно взять чужой телефон, позвонить в службу поддержки оператора и тоже заблокировать SIM-карту как утраченную.

Затраты

Китай — исходная версия. Бесплатно. На всё уйдёт десять с лишним минут.

Выгода

Китай — исходная версия. Порядок важнее скорости. Первый шаг — заблокируйте SIM-карту как утраченную, чтобы другие не могли получать ваши коды подтверждения. Второй шаг — удалённо заблокируйте телефон и удалите всё его содержимое. Третий шаг — с компьютера смените пароли от электронной почты и платёжных сервисов. Четвёртый шаг — заявите в китайскую полицию и получите подтверждение приёма заявления. В конце при необходимости заморозьте банковские карты. Федеральная комиссия по связи США тоже советует удалённо блокировать телефон, даже если вы думаете, что просто потеряли его. Если телефон украли, сразу заявите в полицию, сообщите модель и номер IMEI (идентификационный номер телефона) и немедленно уведомите оператора

Примечания

Китай — исходная версия. Заранее запишите номера служб поддержки трёх китайских операторов: «Китайская мобильная связь» (移动) 10086, «Объединённая связь Китая» (联通) 10010, «Китайские телекоммуникации» (电信) 10000. Запишите также, в каком городе вы оформляли свой номер телефона: служба поддержки спросит об этом. С чужого телефона тоже можно позвонить в службу поддержки и заблокировать SIM-карту как утраченную

Источники

Китай — исходная версия — источники

1. US FCC. Protect Your Smart Device. www.fcc.gov/consumers/guides/protect-your-mobile-device
2. 步骤顺序是作者经验
3. 补办身份证见第 7 节，冒名贷款见第 8 节关于征信的一条

[Предложить правку](#) — ошибка, устаревший закон или лучший источник.

5. Если с карты украли деньги, сначала заявите об утрате и заблокируйте её, затем обратитесь в полицию и потребуйте возмещения от банка: доказать, что «это вы сами совершили операцию», в Китае обязан банк

- Выгодность исходной версии: высокая
- Доказательность А · исходная версия
- для денег
- бесплатно
- мимоходом
- немного силы воли
- Нормы Китая (КНР)
- Аналог в России не найден

Искали в официальных российских источниках (проверено 08.10.2026), прямого аналога не нашли. Это не значит, что его нет. Китайские условия на Россию не переносите.

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Китай — исходная версия. Если в Китае кто-то украл деньги с вашей карты, вам не нужно доказывать, что «эту операцию совершили не вы». Наоборот, банк должен предъявить доказательства, что операцию совершили вы лично. Если не сможет, он должен возместить вам ущерб. Условие — заявить об утрате и заблокировать карту сразу, как только вы обнаружили кражу. Если затянуть с заявлением об утрате, дополнительные потери придётся нести самостоятельно.

Затраты

Китай — исходная версия. Денег не требует. Заметив подозрительные операции по карте, сразу заявите об утрате или заблокируйте её. Сохраните запись об обращении в полицию, запись о заявлении об утрате и уведомления банка об операциях. Если карта всё ещё у вас, поблизости сделайте запрос по карте либо внесите или снимите небольшую сумму. Сохраните запись, чтобы доказать, что в момент происшествия настоящая карта была у вас. Самое трудное — удержаться от спора со службой поддержки и сначала заявить об утрате.

Выгода

Китай — исходная версия. Правила Верховного народного суда (最高法院) разграничивают, кто должен предъявлять доказательства. Если вы утверждаете, что деньги украли с помощью поддельной карты или через интернет, сначала нужно предъявить доказательства. Кража с помощью поддельной карты — это когда кто-то сделал копию вашей карты и расплатился ею. Доказательствами могут служить: вступившие в силу правовые документы, сведения о том, где находилась настоящая карта в момент операции и где совершалась сама операция. А также выписки по счёту, уведомления об операциях, записи об обращении в полицию, записи о заявлении об утрате и так далее. **И наоборот, если банк, выпустивший карту, или небанковская платёжная организация (сторонний платёжный сервис) утверждают, что операцию совершил сам держатель карты либо кто-то с его разрешения, доказательства должны предъявить они.** Если после вашего уведомления банк не провёл своевременную проверку либо вовремя не предоставил или не сохранил документы об операции и записи камер наблюдения, из-за чего доказательства получить невозможно, последствия отсутствия доказательств несёт банк. После подтверждения факта кражи держатель дебетовой карты (карты для хранения собственных денег) может потребовать от банка, выпустившего карту, выплатить украденную сумму вклада с процентами и возместить убытки. Держатель кредитной карты может потребовать вернуть списанную сумму овердрафта с процентами и неустойкой, а также возместить убытки. Если банк, в свою очередь, требует от вас погасить этот овердрафт, суд такое требование не поддержит. Также можно потребовать от банка, выпустившего карту, своевременно удалить соответствующую негативную запись из кредитной истории (по всему Китаю, действует с 25 мая 2021 года)

Примечания

Китай — исходная версия. В двух случаях в Китае ответственность придётся нести самостоятельно. Первый — если вы не обеспечили сохранность банковской карты, пароля, кода подтверждения и тому подобного и в этом есть ваша вина (в оригинале: «не исполнили обязанность по надлежащему обеспечению сохранности и виновны в этом»). Ответственность зависит от степени вины. Поэтому не сообщайте другим пароль и не пересылаете другим коды подтверждения (см. пункт 1: для второго этапа проверки в первую очередь используйте подтверждение во всплывающем окне на телефоне). Второй — если вы вовремя не заявили об утрате и убытки продолжили расти. Дополнительную часть придётся нести самостоятельно. Поэтому первый шаг всегда — заявить об утрате и заблокировать карту, а не звонить в службу поддержки, чтобы спорить. Эти правила распространяются и на сторонние платёжные организации. Если в рекламных материалах такой организации указано «предварительное возмещение», а обещание сформулировано конкретно и ясно, можно на этом основании потребовать, чтобы она сначала возместила ущерб. Если мошенники обманом заставили вас самостоятельно перевести деньги, нужен другой порядок действий. См. раздел 8, пункт 2 (обнаружив обман в Китае, сразу звоните 110 или 96110 и требуйте остановить платёж).

Источники

Китай — исходная версия — источники

1. 最高人民法院 (2021). 关于审理银行卡民事纠纷案件若干问题的规定 (第四、五、七、十四、十五条) . www.court.gov.cn/fabu/xiangqing/304771.html

[Предложить правку](#) — ошибка, устаревший закон или лучший источник.

6. Время от времени проверяйте устройства, на которых выполнен вход в ваш аккаунт, и приложения с предоставленным доступом. Удаляйте те, которыми не пользуетесь

- Выгодность исходной версии: обычная
- Доказательность С · исходная версия
- для денег
- бесплатно
- мимоходом
- немного силы воли
- Частично Китай
- Аналог в России не найден

Искали в официальных российских источниках (проверено 08.10.2026), прямого аналога не нашли. Это не значит, что его нет. Китайские условия на Россию не переносите.

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Китай — исходная версия. «Устройства, на которых выполнен вход» — это телефоны и компьютеры, с которых сейчас всё ещё можно пользоваться вашим аккаунтом. Те, кто крадёт аккаунты, часто сначала какое-то время выжидают и только потом действуют. Если в списке появилось незнакомое вам устройство или к аккаунту всё ещё подключена программа, которой вы давно не пользуетесь, сразу выйдите из аккаунта на всех устройствах, а затем смените пароль.

Затраты

Китай — исходная версия. Бесплатно. Каждая проверка занимает несколько минут. Сложность в том, что никто не напоминает: нужно самим помнить о проверке.

Выгода

Китай — исходная версия. При краже аккаунта злоумышленник часто действует не сразу, а сначала какое-то время выжидает. В списке устройств, на которых выполнен вход в аккаунт, указаны телефоны и компьютеры, с которых сейчас всё ещё можно пользоваться этим аккаунтом. В списке приложений с предоставленным доступом указаны сторонние программы, которым вы разрешили входить через этот аккаунт. Незнакомые устройства и сторонние программы, которыми вы давно не пользуетесь, — самые легко заметные следы

Примечания

Китай — исходная версия. Такой раздел есть в приложениях «Вичат» (微信) и «Алипэй» (支付宝), в электронной почте, в аккаунтах Apple и Android. Если обнаружите незнакомое устройство, нажмите «Выйти из аккаунта на всех устройствах», а затем смените пароль

Источники

Китай — исходная версия — источники

1. 作者经验，无直接文献

[Предложить правку](#) — ошибка, устаревший закон или лучший источник.

7. Не нажимайте «Согласиться со всем» ради использования приложения: если информация не обязательна, вам в Китае не могут отказать в услуге даже без вашего согласия

- Выгодность исходной версии: обычная
- Доказательность А · исходная версия
- для свободы
- бесплатно
- мимоходом
- немного силы воли
- Частично Китай
- Российские данные: частично

Китайские условия и российские данные разделены по полям. Российская сверка частичная; непроверенные поля отмечены отдельно. Оценки и фильтры относятся к исходной версии.

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Китай — исходная версия. Если в Китае приложение запрашивает вашу информацию, которая не нужна для предоставления этой услуги, оно не может запретить вам пользоваться им из-за того, что вы не согласились её предоставить. Сбирать оно тоже может только ту информацию, которая нужна. Карте необходимо ваше местоположение, а фонарику ваши контакты не нужны.

Россия. В России организация тоже не вправе отказывать в услуге только потому, что человек не предоставил персональные или биометрические данные. Исключение — данные, которые нужно предоставить по закону или которые напрямую связаны с исполнением договора. В выдержках нет общего правила о сборе только минимально необходимого объёма данных.

Затраты

Китай — исходная версия. Бесплатно. Трудно удержаться и не нажать «Согласиться со всем».

Россия. В этих источниках цена не указана.

Выгода

Китай — исходная версия. В китайском законе прямо прописаны два правила. Первое: нельзя отказывать в предоставлении продукта или услуги на том основании, что человек не согласился или отозвал согласие; исключение — когда обработка этой информации необходима для

предоставления услуги. Второе: сбор должен ограничиваться минимальным объёмом, необходимым для достижения цели обработки; собирать можно только ту информацию, которая нужна

Россия. Можно отказаться от необязательных персональных и биометрических данных без отказа в услуге или обслуживании.

Примечания

Китай — исходная версия. Критерий — необходима ли эта информация для предоставления этой услуги. Карте нужно местоположение, а фонарику контакты не нужны. После установки приложения сначала откройте страницу разрешений приложений в настройках телефона и отключите ненужные разрешения. Когда они действительно понадобятся, выберите «Разрешить только в этот раз».

Россия. Российские выдержки говорят об отказе в услуге и обслуживании, но не подтверждают правило о минимальном сборе данных приложением.

Источники

Китай — исходная версия — источники

1. 全国人大常委会 (2021). 个人信息保护法. 中国人大网.
www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html: 第六条「收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息」
2. 第十六条「个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外」
3. 第十五条「基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式」

Россия — источники

1. Федеральные - Роспотребнадзор. Проверено 08.10.2026.
zpp.rosпотребнадзор.ru/news/federal/479701

[Предложить правку](#). — ошибка, устаревший закон или лучший источник.

8. Вы имеете право просматривать, копировать, исправлять и удалять свои персональные данные, а при отказе можете подать в суд (в Китае)

- Выгодность исходной версии: обычная
- Доказательность A · исходная версия
- для свободы
- бесплатно
- мимоходом
- немного силы воли
- Частично Китай
- Аналог в России не найден

Искали в официальных российских источниках (проверено 08.10.2026), прямого аналога не нашли. Это не значит, что его нет. Китайские условия на Россию не переносите.

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Китай — исходная версия. Вы имеете право требовать от компании дать вам возможность просматривать, копировать, исправлять и удалять свои данные. Если оказание услуги прекращено, срок хранения истёк или вы отозвали согласие, компания и так должна удалить их сама. Если она отказывает вам, то обязана объяснить причины. Если не выполняет требование, вы можете сразу подать на неё в суд. Удаление учётной записи и удаление данных — две разные вещи. После удаления учётной записи нужно отдельно потребовать удаления данных.

Затраты

Китай — исходная версия. Бесплатно. Жаловаться или подавать в суд нужно только в том случае, если другая сторона затягивает дело. Если действительно дойдёт до суда, это займёт как минимум несколько месяцев, а адвоката придётся оплачивать самостоятельно. Поэтому сначала подать жалобу выгоднее. Трудность в том, что при затягивании приходится снова и снова напоминать о своём требовании.

Выгода

Китай — исходная версия. Есть несколько случаев, когда компания должна сама удалить данные: оказание услуги прекращено, согласованный срок хранения истёк, вы отозвали согласие, первоначальная цель сбора данных уже достигнута и так далее. Если она их не удалила, вы можете потребовать удаления. Если она отказывает вам в осуществлении этих прав, то обязана объяснить причины. Вы можете сразу обратиться в суд.

Примечания

Китай — исходная версия. Удаление учётной записи и удаление персональных данных — две разные вещи. После удаления учётной записи нужно отдельно потребовать удаления данных. Прежде чем сменить телефон или продать старый, сначала выйдите на старом телефоне из всех учётных записей и отвяжите их от него, а затем сбросьте телефон до заводских настроек. Закон даёт вам право на удаление данных постфактум. Он не может за вас вернуть данные, которые уже утекли.

Источники

Китай — исходная версия — источники

1. 全国人大常委会 (2021). 个人信息保护法. 中国人大网.
www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html: 第四十五条「个人有权向个人信息处理者查阅、复制其个人信息……个人请求查阅、复制其个人信息的, 个人信息处理者应当及时提供」
2. 第四十六条更正、补充权

3. 第四十七条列了五种应当主动删除的情形，含「（一）处理目的已实现、无法实现或者为实现处理目的不再必要」「（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满」「（三）个人撤回同意」，「个人信息处理者未删除的，个人有权请求删除」
4. 第五十条「个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由」「个人可以依法向人民法院提起诉讼」

[Предложить правку](#) — ошибка, устаревший закон или лучший источник.

9. Вы не обязаны соглашаться на распознавание лица в Китае: если есть другой способ, нельзя требовать только распознавание лица; если вы не согласны, вам должны предложить другой способ

- Выгодность исходной версии: обычная
- Доказательность А · исходная версия
- для денег
- бесплатно
- мимоходом
- немного силы воли
- Нормы Китая (КНР)
- Аналог в России не найден

Искали в официальных российских источниках (проверено 08.10.2026), прямого аналога не нашли. Это не значит, что его нет. Китайские условия на Россию не переносите.

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Китай — исходная версия. Если ту же задачу можно решить другим способом, нельзя требовать от вас только распознавания лица. Если вы не согласны, вам должны предложить другой способ: карту, пароль или удостоверение личности. Нельзя заставлять вас соглашаться словами «тогда мы не сможем вас обслужить». В гостиничных номерах, общественных банях, раздевалках и туалетах никому нельзя устанавливать оборудование для распознавания лиц.

Затраты

Китай — исходная версия. Денег не нужно. Когда требуют пройти распознавание лица, спросите: «Есть ли другой способ проверки?» Если говорят, что нет, потребуйте его предоставить. Самое трудное — спросить об этом лично.

Выгода

Китай — исходная версия. В «Мерах по управлению безопасностью применения технологий распознавания лиц (人脸识别技术应用安全管理办法)» прямо сказано: «Если существуют другие способы, не использующие технологию распознавания лиц, которые позволяют достичь той же цели или выполнить те же требования к обслуживанию, запрещается использовать технологию распознавания лиц как единственный способ проверки. Если человек не согласен на проверку

личности по информации о его лице, необходимо предоставить другие разумные и удобные способы». В Мерах также сказано: «Никаким организациям и частным лицам нельзя под предлогом предоставления услуг, повышения качества обслуживания и тому подобного вводить человека в заблуждение, обманывать или принуждать его соглашаться на проверку личности с помощью технологии распознавания лиц». Если информацию о вашем лице обрабатывают на основании вашего согласия, необходимо получить «отдельное согласие, данное добровольно и явно при условии полной информированности»: вас должны отдельно спросить именно об этом, и только ваше отдельное согласие считается действительным. Вы вправе отозвать согласие, а тот, кто обрабатывает информацию, должен предоставить удобный способ его отзыва. Для обработки информации о лице несовершеннолетнего младше 14 лет необходимо получить согласие родителей или других опекунов. Установка оборудования для распознавания лиц в общественных местах «должна быть необходима для обеспечения общественной безопасности» и сопровождаться заметными предупреждающими обозначениями. Никаким организациям и частным лицам нельзя устанавливать такое оборудование внутри частных пространств в общественных местах: гостиничных номеров, общественных бань, общественных раздевалок, общественных туалетов и тому подобных мест. Информация о лицах должна храниться в самом оборудовании для распознавания лиц, передавать её вовне через интернет запрещено. Есть два исключения: если законами или административными нормативными актами предусмотрено иное либо получено отдельное согласие (по всему Китаю, действует с 1 июня 2025 года)

Примечания

Китай — исходная версия. Чаще всего записать данные вашего лица требуют для прохода в жилой комплекс, на платформах аренды жилья, в спортзалах и гостиницах. Когда вам говорят: «Система поддерживает только распознавание лица», прочитайте им точную формулировку из Мер. Она звучит так: «Если существуют другие способы, не использующие технологию распознавания лиц, которые позволяют достичь той же цели или выполнить те же требования к обслуживанию, запрещается использовать технологию распознавания лиц как единственный способ проверки». Затем потребуйте предоставить другой способ: карту, пароль или удостоверение личности. Если его по-прежнему не предоставляют, сообщите об этом в местный орган по вопросам интернета и информатизации (网信部门). Если государство в Китае установило иные правила проверки личности по лицу, например для некоторых финансовых операций и государственных услуг, нужно следовать этим правилам. Главное отличие лица от пароля в том, что после утечки его нельзя изменить, поэтому с ним стоит быть осторожнее, чем с паролем. Организации, хранящие информацию о лицах 100 тыс. человек и более, должны в течение 30 рабочих дней зарегистрировать это в органе по вопросам интернета и информатизации уровня провинции или выше (省级以上网信部门). Об этом тоже можно спросить, чтобы понять, соблюдает ли организация правила. О праве просматривать, исправлять и удалять свои персональные данные см. пункт 8. Если кто-то использует ваше лицо, чтобы оформить свой кредит, это другая ситуация, см. раздел 8, пункт [45](#) (помощь с распознаванием лица).

Источники

Китай — исходная версия — источники

1. 国家互联网信息办公室、公安部 (2025). 人脸识别技术应用安全管理办法 (第 19 号令, 第十条、十二条、十三条, 2025 年 6 月 1 日起施行). www.cac.gov.cn/2025-03/21/c_1744174262156096.htm

[Предложить правку](#) — ошибка, устаревший закон или лучший источник.

10. Не передавайте код, ключи и личные данные «AI-посредникам» неизвестного происхождения, особенно когда AI автоматически выполняет команды

- Выгодность исходной версии: обычная
- Доказательность В · исходная версия
- для свободы
- немного денег
- мимоходом
- немного силы воли
- Частично Китай
- Аналог в России не найден

Искали в официальных российских источниках (проверено 08.10.2026), прямого аналога не нашли. Это не значит, что его нет. Китайские условия на Россию не переносите.

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Китай — исходная версия. Посредник стоит между вами и поставщиком модели. Он видит и может менять все, что вы отправляете, и все ответы, которые получаете. В одном исследовании проверили более 400 посредников: 9 вставляли в ответы вредоносный код, а 17 использовали ключи облачных сервисов, которые исследователи специально туда поместили. Если AI автоматически выполняет команды, одной измененной команды достаточно, чтобы компьютер оказался под чужим контролем.

Затраты

Китай — исходная версия. Прямое подключение к официальному сервису обычно дороже, чем через посредника, и пополнять баланс не так удобно. Сложность в том, что посредники дешевы, а через одну точку входа можно обращаться к моделям нескольких компаний

Выгода

Китай — исходная версия. Министерство государственной безопасности (国家安全部) в июне 2026 года опубликовало предупреждение о рисках. Некоторые посредники сохраняют присланные пользователями данные на своих серверах. Некоторые без разрешения удерживают их и перепродают другим поставщикам больших моделей для обучения. Некоторые скрывают в своих сервисах бэкдоры, внедряют вредоносный код на устройства пользователей, крадут ключи учетных записей и учетные данные для доступа к облачным сервисам, даже устанавливают программы удаленного управления. В предупреждении рекомендуется подключаться напрямую к официальным сервисам или пользоваться платформами с надлежащей авторизацией, а не платформами неизвестного происхождения, без разрешения на ведение деятельности и без гарантий безопасности. Перед использованием нужно обезличить личные данные и материалы проектов, надежно хранить ключи и регулярно менять их. При неожиданных списаниях, блокировке учетной записи без причины или аномалиях с данными нужно немедленно прекратить использование, сменить ключи, проверить устройство на вирусы и удалить их, сохранить доказательства. В 2026 году исследователи из Калифорнийского университета в Санта-Барбаре и других организаций провели измерительное исследование. Они купили доступ к 28 платным

посредникам на китайской торговой площадке (淘宝), на китайской площадке продажи поддержанных товаров (闲鱼) и в зарубежных интернет-магазинах, а также собрали в открытых сообществах 400 бесплатных посредников. Оказалось, что 1 платный и 8 бесплатных посредников внедряли вредоносный код в возвращаемые вызовы инструментов. Вызов инструмента — это команда, которую AI дает вашему компьютеру, например для установки программного пакета. Еще 2 выбирали момент для атаки. В статье приведен пример: атаковали только сеансы с полностью автоматическим выполнением команд. 17 использовали ключи облачных сервисов Amazon, которые исследователи специально туда поместили. 1 вывел деньги из Ethereum-кошелька исследователей. В кошельке было совсем мало денег, потери составили менее 50 долларов США. Показанная в статье подмена очень незаметна: в команде установки requests заменяют на похожее по написанию reqeusts, и с первого взгляда этого не видно (по всему Китаю)

Примечания

Китай — исходная версия. Уровень В присвоен потому, что исследование только одно, и это препринт, то есть версия, выложенная до официальной публикации. Большинство проверенных посредников были бесплатными, платных было только 28, поэтому нельзя вычислить, «какая доля посредников имеет проблемы». Некоторые СМИ написали, что в том случае украли 500000 долларов США, но в самой статье указано менее 50 долларов США. Масштаб выгоды оценен как средний, исходя из последствий: размер потерь от кражи ключей и кода может сильно различаться, а в исследовании нет суммы, которую можно было бы взять за основу. Если вы уже пользовались посредником неизвестного происхождения, отзовите использованные ключи у поставщика модели и создайте новые. Заодно замените ключи облачных сервисов и репозиторий кода. При работе через посредника не позволяйте AI выполнять команды полностью автоматически: сначала просмотрите команду и только потом разрешайте выполнение. Сторона, управляющая посредническим сервисом, рискует столкнуться с уголовной ответственностью в Китае, см. раздел 11, пункт [19](#) (AI-посредники). Кому это выгодно — вам самим.

Источники

Китай — исходная версия — источники

1. 国家安全部 (2026). 「AI中转站」, 风险要防范.
www.szzg.gov.cn/2026/xwzx/szqx/202606/t20260608_5331487.htm (数字中国建设峰会官网 转载国家安全部微信公众号)
2. Liu H, Shou C, Wen H, Chen Y, Fang RJ, Feng Y. (2026). Your Agent Is Mine: Measuring Malicious Intermediary Attacks on the LLM Supply Chain. arXiv:2604.08407.
arxiv.org/abs/2604.08407

[Предложить правку](#) — ошибка, устаревший закон или лучший источник.