

ПАМЯТКА 10

Установил приложение или дал удалённый доступ



Учебная иллюстрация

В этом случае одного закрытия сайта недостаточно. Считайте устройство недоверенным до проверки и используйте другой безопасный телефон или компьютер для банка и смены важных секретов.

Цифровая безопасность · Иван Юрьевич · Версия 1.0 · Редакционная проверка: 2026-10-26

Как понять, что случилось

- По просьбе собеседника установлены приложение, расширение, профиль управления либо программа удалённой помощи. Были выданы специальные разрешения, доступ к экрану, уведомлениям или управлению устройством.
- Курсор движется сам, экран видит посторонний, защита отключена либо появились неизвестные приложения. Не все угрозы заметны: отсутствие таких признаков не подтверждает чистоту.

Что сделать сейчас

1. Остановите сеанс удалённого управления и отключите подозрительное устройство от сети: Wi-Fi, мобильные данные или кабель. Это ограничивает связь, но не доказывает удаление угрозы.
2. С другого безопасного устройства немедленно свяжитесь с банком, если использовались банковские приложения, передавались коды или демонстрировался экран. Попросите проверить доступ и необходимые ограничения.
3. С безопасного устройства защитите основную почту и важные аккаунты: смените раскрытые пароли, проверьте резервные контакты, отзовите посторонние сеансы и разрешения.
4. Сохраните название программы, время установки и сведения о разговоре без повторного запуска. Если это рабочее устройство, сообщите администратору и следуйте его порядку.

Что дальше

- Обратитесь к доверенному специалисту или официальной поддержке производителя. Проверьте установленные программы, расширения, специальные разрешения, профили и средства защиты; один удалённый значок не означает очистку.
- При необходимости выполните переустановку или сброс по официальной инструкции после сохранения нужных файлов и проверки восстановления. Не переносите подозрительные приложения обратно из копии.
- Проверьте операции и сообщения после возврата контроля. Сохраните доказательства для банка и полиции; результат антивируса не отменяет необходимость проверки уже раскрытых секретов.

Чего не делать

- Не вводите новые пароли и банковские коды на подозрительном устройстве. Не соглашайтесь на ещё одну удалённую сессию от человека, который первым предложил «исправить взлом».
- Не переустанавливайте систему до обсуждения сохранения доказательств и копий, если это может помешать расследованию. Не обещайте себе, что приложение из магазина автоматически безопасно.

Ваш вариант ситуации

Android или iPhone

- Особенно проверьте специальные возможности, администрирование, профили управления и доступ к экрану. Набор разделов зависит от системы; используйте справку производителя, не выдуманный универсальный путь.

Windows

- Проверьте программы удалённого доступа и расширения. Штатная и автономная проверка защиты полезны, но при сомнениях решение об очистке принимает специалист.

Официальная помощь

- [Microsoft: нежелательные программы](https://support.microsoft.com) support.microsoft.com
- [Банк: срочные действия](https://www.tbank.ru) www.tbank.ru

Версия 1.0. Редакционная проверка 2026-10-26. Читайте эту памятку на learn.ivan-it.net/memos/suspicious-app.

Связанные уроки: [Телефон, компьютер и домашняя сеть](#); [Если уже случилось](#).

Источники: [Microsoft: Защита компьютера от нежелательных программ](#) (проверка 2026-10-26); [Microsoft: Защита от вирусов и угроз в Безопасности Windows](#) (проверка 2026-10-26); [Т-Банк: Что делать, если перевели деньги мошенникам](#) (проверка 2026-10-26).

Возможности сервисов меняются; результат восстановления и возврат денег не гарантируются. При риске денег немедленно обращайтесь в свой банк. Учебный сайт не заменяет официальную поддержку.