

ПАМЯТКА 12

Компьютер заблокирован или файлы зашифрованы



Учебная иллюстрация

Отделите пугающее окно браузера от настоящей блокировки системы или изменения файлов. Сначала ограничьте распространение и сохраните сведения; не подключайте резервные носители к подозрительному компьютеру.

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

Как понять, что случилось

- Файлы перестали открываться, изменились их расширения, появилась записка с выкупом или защита сообщила о шифровальщике. Это отличается от одной полноэкранной страницы со звуком и телефоном «поддержки».
- Общие папки и подключённые диски тоже недоступны. На рабочем компьютере не проводите самостоятельное лечение: такие признаки необходимо сразу сообщить ответственному администратору.

Что сделать сейчас

1. Отключите подозрительный компьютер от сети и общих ресурсов: выньте сетевой кабель и отключите Wi-Fi. Не подключайте к нему диски с резервными копиями и другие устройства.
2. Если это компьютер организации, немедленно свяжитесь с администратором с другого устройства. Для домашнего компьютера найдите доверенного специалиста; сообщите, продолжается ли изменение файлов.
3. Сфотографируйте сообщение и запишите время, не открывая ссылки и приложения из записки. Сохраняйте оригиналы зашифрованных файлов: они могут понадобиться специалисту и для будущей проверки восстановления.
4. Если раскрыты банковские данные или удалённо управляли компьютером, сразу свяжитесь с банком с другого безопасного устройства. Не входите в банк на заражённой системе.

Что дальше

- Специалист поможет установить масштаб, остановить угрозу и выбрать безопасную переустановку либо другой порядок. Проверка защиты полезна, но не гарантирует возвращение зашифрованных данных.
- После очистки проверьте резервную копию до восстановления. Используйте версию, созданную до происшествия; синхронизированная папка могла успеть получить уже испорченные файлы.
- С безопасного устройства смените скомпрометированные пароли, проверьте сеансы почты и связанные аккаунты. Сохраните доказательства и при преступлении обратитесь в полицию.

Чего не делать

- Не платите по обещанию гарантированной расшифровки и не загружайте случайный «дешифратор». Не форматируйте диски и не удаляйте записку до согласования с помогающим специалистом.
- Не пытайтесь проверить резервную копию, подключая её к заражённой системе. Не называйте чистой систему лишь потому, что исчезло предупреждение или один сканер не нашёл угроз.

Ваш вариант ситуации

Только окно в браузере

- Не звоните по показанному номеру и не разрешайте удалённую помощь. Закройте вкладку или браузер штатно, затем проверьте систему; не нажимайте кнопки внутри пугающей страницы.

Зашифрованы общие файлы

- Прекратите использование общих дисков и предупредите остальных владельцев. В рабочей сети решение об изоляции и сохранении памяти принимает администратор, исходя из ситуации.

Официальная помощь

- [Microsoft: защита от угроз](https://support.microsoft.com/ru-ru/windows/защита-от-угроз) support.microsoft.com
- [Microsoft: нежелательные программы](https://support.microsoft.com/ru-ru/windows/нежелательные-программы) support.microsoft.com

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

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

Источники: [Microsoft: Защита от вирусов и угроз в Безопасности Windows](#) (проверка 2026-10-26); [Microsoft: Защита компьютера от нежелательных программ](#) (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.