

Массовый бойкот заставил компанию отказаться от спорной концепции «предустановленного шпионского ПО».

Компания Microsoft — это американская многопрофильная компания, занимающаяся разработкой программного обеспечения и производством компьютерной техники. Она была основана в 1975 году Биллом Гейтсом и Полом Алленом и на сегодняшний день является одной из самых крупных и известных IT-компаний в мире. Среди продуктов Microsoft наиболее известными являются операционные системы Windows, пакеты офисных приложений Office, браузер Internet Explorer и поисковая система Bing. Кроме того, компания занимается разработкой программного обеспечения для серверов, баз данных, игровых консолей Xbox и многих других устройств. Microsoft также предоставляет услуги облачных вычислений и хранения данных через свою платформу Azure, а также занимается разработкой искусственного интеллекта и других инновационных технологий. Компания имеет филиалы по всему миру и сотрудничает с многими крупными корпорациями и организациями." data-html="true" data-original-title="Microsoft" >Microsoft объявила, что не станет в принудительном порядке включать всем пользователям спорную функцию Recall, основанную на искусственном интеллекте. Активация новой технологии отныне будет производиться исключительно по желанию пользователя.

Функция Recall, находящаяся сейчас на стадии предварительного тестирования и предназначенная для Copilot+ PC, делает скриншоты экрана каждые пять секунд, анализируя их для выделения релевантной информации. Официальный запуск функции изначально планировался на 18 июня 2024 года.

Задуманная как ИИ-подобная фотографическая память, функция Recall вызвала мгновенную критику со стороны сообщества безопасности и конфиденциальности. Специалисты осудили компанию за недостаточные меры защиты, которые могли бы предотвратить доступ злоумышленников к цифровой жизни пользователей.

Несмотря на заверения Microsoft о том, что снимки Recall хранятся и обрабатываются локально на устройстве и не передаются другим компаниям или приложениям, шквал негодования пользователей от этого не уменьшился.

Записываемая информация может включать скриншоты документов, электронных писем или сообщений, содержащих конфиденциальные данные. Журналист издания WIRED Энди Гринберг и вовсе назвал Recall «непрощенным предустановленным шпионским ПО», встроенным в новые компьютеры на базе Windows.

Более того, этичный хакер Алекс Хагенах ранее уже представил инструмент TotalRecall собственной разработки, демонстрирующий, насколько легко при желании извлечь все данные из этой локальной базы, хранящейся без шифрования в виде обычного текста.

Для смягчения критики Microsoft сообщила, что пользователи смогут полностью контролировать новую функцию. Кроме того, компания уже ввела ряд изменений безопасности, а также новый процесс первоначальной настройки Recall, позволяющий пользователям полностью отказаться от периодического создания скриншотов.

Изменения в безопасности также включают регистрацию пользователей для биометрического сканирования Windows Hello с необходимостью подтверждения присутствия владельца устройства для просмотра временной шкалы и выполнения поисков по ней.

Кроме того, компания всё же добавила шифрование базы данных поискового индекса, а также отметила, что снимки Recall будут расшифрованы и доступны только после аутентификации пользователя в системе.

Пользователи могут в любой момент приостановить, отфильтровать и удалить сохранённые данные. Для пользователей на управляемых рабочих устройствах в корпоративных средах IT-администраторы могут отключить Recall, хотя не могут включить её самостоятельно.

«Протесты пользователей оказались эффективными», — сказал исследователь безопасности Кевин Бомонт, критиковавший первоначальную реализацию Recall. «Возможность добровольного выбора спасёт многих пользователей от проблем с безопасностью в будущем. Подобные функции никогда не следует включать по умолчанию».