Исследование поставило под сомнение безопасность популярных VPN для Android: многие приложения не защищают данные пользователей

Дата публикации: 08.07.2026

Виртуальные частные сети давно стали одним из самых популярных инструментов для защиты конфиденциальности в интернете. Миллионы пользователей устанавливают VPN-приложения, рассчитывая скрыть свой IP-адрес, зашифровать интернет-трафик и защитить личные данные от постороннего наблюдения. Однако новое исследование американских специалистов показывает, что реальный уровень безопасности многих мобильных VPN-сервисов может существенно отличаться от заявленного разработчиками.

Ученые инженерного факультета Мичиганского университета разработали новую автоматизированную систему анализа безопасности мобильных VPN под названием MVPNalyzer. С ее помощью исследователи провели масштабную проверку популярных приложений для Android и обнаружили многочисленные проблемы, связанные с конфиденциальностью, шифрованием и передачей

пользовательских данных. Результаты исследования были представлены на международном симпозиуме по сетевой и распределенной безопасности NDSS 2026.

Главной особенностью новой платформы стало то, что она впервые позволяет проводить комплексный аудит мобильных VPN-приложений в автоматическом режиме и в большом масштабе. До настоящего времени большинство исследований касалось настольных VPN-сервисов или ограничивалось анализом небольшого количества отдельных приложений. Безопасность мобильных решений оставалась значительно менее изученной, несмотря на то что именно смартфоны сегодня являются основным устройством для выхода в интернет у миллиардов людей.

В ходе исследования специалисты протестировали 281 популярное VPN-приложение для операционной системы Android. Полученные результаты оказались весьма тревожными. Оказалось, что часть сервисов не обеспечивает даже базовый уровень защиты, а некоторые фактически нарушают собственные обещания по обеспечению конфиденциальности.

Одной из наиболее серьезных проблем стали утечки сетевого трафика. Анализ показал, что 29 протестированных VPN допускали утечку DNS-запросов и браузерного трафика. В подобных ситуациях часть интернет-активности пользователя оказывается доступной сторонним наблюдателям, несмотря на включенный VPN. Это сводит к минимуму саму цель использования подобных сервисов, поскольку реальные посещаемые сайты и сетевые запросы могут быть раскрыты.

Еще одной неожиданной находкой стало наличие большого количества незашифрованных соединений. Исследователи обнаружили, что более 20% протестированных приложений передавали часть данных без должного шифрования. Среди такой информации встречались конфигурационные файлы, служебные данные, а в некоторых случаях — сведения, позволяющие определить приблизительное местоположение пользователя. Передача подобных данных в открытом виде значительно повышает риск их перехвата злоумышленниками при использовании небезопасных сетей.

Не менее серьезной проблемой оказалась передача информации третьим лицам. Исследование показало, что 76 VPN-приложений отправляли рекламные идентификаторы устройств и другие уникальные параметры смартфонов сторонним сервисам. Подобные идентификаторы позволяют длительное время отслеживать конкретное устройство независимо от изменения IP-адреса, что противоречит заявлениям многих разработчиков о полной анонимности пользователей.

Особое внимание ученые уделили настройкам криптографической защиты. Им удалось получить конфигурационные файлы 108 VPN-приложений. Практически во всех случаях были обнаружены отклонения от современных рекомендаций по настройке безопасных соединений. Многие сервисы использовали устаревшие криптографические алгоритмы, недостаточно надежные параметры шифрования или неполную аутентификацию соединений. Подобные ошибки могут значительно снижать устойчивость VPN к современным методам атак.

Разработанная система MVPNalyzer отличается от традиционных инструментов анализа тем, что одновременно исследует сразу несколько уровней работы приложения. Она проверяет правильность маршрутизации сетевого трафика, анализирует криптографические параметры, изучает конфигурационные файлы, отслеживает передачу пользовательских данных сторонним сервисам и оценивает устойчивость VPN к различным сценариям обнаружения и блокировки.

Фактически MVPNalyzer выполняет комплексную проверку, включающую сразу несколько направлений: анализ туннелирования сетевого трафика, оценку качества шифрования, проверку конфигураций безопасности, контроль передачи пользовательских данных, выявление утечек информации, исследование взаимодействия с внешними серверами.

Подобный подход позволяет обнаруживать проблемы, которые практически невозможно выявить при обычном пользовательском тестировании. Многие приложения успешно создают VPN-соединение и внешне работают корректно, однако часть критически важного трафика продолжает передаваться в обход защищенного канала или отправляется сторонним сервисам без ведома пользователя.

Исследование вновь поднимает вопрос о доверии к VPN-индустрии. Большинство пользователей не имеют технической возможности самостоятельно проверить, действительно ли приложение выполняет заявленные функции. При выборе сервиса люди часто ориентируются на рекламные обещания, количество загрузок или пользовательские оценки, которые далеко не всегда отражают реальный уровень безопасности.

Авторы работы считают, что подобные инструменты автоматизированного аудита могут стать важным элементом регулирования рынка цифровой безопасности. Их использование позволит государственным органам, независимым лабораториям и организациям по защите прав потребителей регулярно проводить объективную оценку качества VPN-приложений и формировать единые стандарты безопасности.

Не менее полезной новая система может оказаться и для самих разработчиков. Регулярное использование подобных инструментов позволит выявлять ошибки еще до публикации обновлений, устранять потенциальные уязвимости и повышать доверие пользователей к собственным продуктам.

Исследователи также отмечают, что возможности MVPNalyzer не ограничиваются только VPN-сервисами. Архитектура платформы позволяет адаптировать ее для анализа других приложений, работающих с конфиденциальной информацией. В будущем подобные методы могут использоваться для проверки безопасности мессенджеров, финансовых сервисов, медицинских платформ, корпоративных приложений и других программ, через которые ежедневно передаются персональные данные миллионов пользователей.

Полученные результаты еще раз подтверждают, что наличие VPN само по себе не гарантирует защиту информации. Реальный уровень безопасности зависит от качества реализации приложения, используемых криптографических технологий и добросовестности разработчиков. Новое исследование демонстрирует необходимость более прозрачного контроля цифровых сервисов и показывает, что регуляримый независимый аудит становится важной частью современной кибербезопасности в условиях стремительного роста мобильных технологий.

Ссылка: «MVPNalyzer: Исследовательская структура для аудита безопасности и конфиденциальности мобильных VPN, Труды Симпозиума по безопасности сетей и распределенных систем 2026 года» DOI: 10.14722/ndss.2026.231573.