УДК 004

Тактаев Т.У.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

ПРИВАТНОСТЬ В МЕССЕНДЖЕРАХ: НАСКОЛЬКО ЗАЩИЩЕНЫ НАШИ ПЕРЕПИСКИ?

Аннотация. В статье рассматриваются современные угрозы приватности в мессенджерах, методы их защиты, включая сквозное и постквантовое шифрование, а также концепция мессенджера нового поколения. Отдельное внимание уделено проблеме сбора метаданных и децентрализации. Представлены предложения по созданию мессенджера, обеспечивающего максимальную безопасность и конфиденциальность общения.

Ключевые слова: приватность, мессенджеры, шифрование, метаданные, безопасность.

Современные мессенджеры применяют E2EE как стандарт шифрования, но метаданные остаются уязвимыми. Signal считается самым безопасным, тогда как Telegram критикуется за непрозрачность. TLS защищает передачу данных, но не исключает их хранения. Даже защищенные мессенджеры, такие как Signal или Briar, собирают метаданные, позволяющие анализировать поведение пользователей. Централизованные серверы создают риски взломов и утечек, что подтверждают случаи с Telegram и WhatsApp.

Развитие квантовых технологий ставит под угрозу текущие алгоритмы шифрования, требуя перехода на постквантовые решения. Приватность одновременно защищает пользователей от внешних угроз и может использоваться злоумышленниками для сокрытия противоправной деятельности. Необходим баланс между безопасностью и контролем.

Приватные каналы могут быть использованы для координации преступных схем, распространения запрещенного контента или даже террористических действий, поскольку отсутствие контроля и прозрачности создает пространство для злоупотреблений.

Найти оптимальный баланс между защитой персональных данных и предотвращением злоупотреблений – сложная, но необходимая задача. Вот несколько ключевых направлений для решения данной проблемы:

1. Технологическая гибкость: Разработка мессенджеров и систем связи, которые позволят пользователю самостоятельно регулировать уровень приватности в зависимости от ситуации. Например, возможность выбора

между режимами высокой анонимности и режимами, где предусмотрено определенное логирование для оперативного реагирования на угрозы.

2. Интеграция аналитических инструментов: Использование искусственного интеллекта для выявления аномалий в поведении пользователей без нарушения их приватности. Такие системы могут предупреждать о подозрительной активности, не раскрывая личную информацию законопослушных пользователей.

3. Децентрализация: Разработка децентрализованных архитектур, где контроль над данными остается у пользователя, а не централизованных сервисов, что минимизирует риск их незаконного использования, но при этом затрудняет злоумышленникам организацию скрытых групповых сетей.

4. Регуляция и стандартизация: Формирование нормативных актов, устанавливающих границы допустимой приватности в цифровых коммуникациях. Законодательное регулирование может помочь в определении рамок, в которых приватность остается инструментом защиты, а не средством для укрытия преступной деятельности.

Для обеспечения истинной приватности необходимо:

- минимизация сбора данных: отказ от логирования активности пользователей;
- защита метаданных: использование луковой маршрутизации и микс-сетей;
- полный контроль пользователя: гибкие настройки конфиденциальности;
- постквантовое шифрование: защита от будущих угроз;
- децентрализованные идентификаторы: отказ от привязки к телефонным номерам.

Такая архитектура обеспечит максимальную приватность, устойчивость к цензуре и защиту от потенциальных атак.

Для защиты метаданных предлагаются следующие решения:

- луковая маршрутизация – передача сообщений через несколько узлов, скрывающая отправителя и получателя;
- обфускация трафика – создание фонового трафика, затрудняющего анализ данных;
- децентрализованная серверная архитектура – устранение единой точки отказа.

Для защиты от квантовых атак необходимо внедрение постквантовой криптографии. Среди перспективных алгоритмов – Kyber и хеш-базированные подписи. Важно учитывать их эффективность на мобильных устройствах.

Пользовательский контроль будет включать:

- гибкую настройку анонимности в зависимости от уровня риска;
- опции самоуничтожающихся сообщений с различными таймерами;
- интуитивные индикаторы уровня безопасности в чатах;

- использование блокчейна и AI для повышения безопасности.
- блокчейн обеспечит децентрализованную идентификацию без телефонных номеров и прозрачность хранения данных;
- AI может анализировать аномалии в доступе к данным, выявлять утечки и повышать безопасность, не нарушая приватности.

Эти технологии помогут создать мессенджер, обеспечивающий беспрецедентный уровень конфиденциальности и безопасности.

Существующие децентрализованные мессенджеры (Signal, Session, Briar, Matrix) предлагают частичную защиту приватности, но сталкиваются с проблемами удобства, масштабируемости и защиты метаданных.

Для создания максимально защищенного мессенджера необходимо объединить их сильные стороны:

- децентрализация – устранение единых точек отказа;
- постквантовое шифрование – защита от будущих угроз;
- луковая маршрутизация и микс-сети – скрытие метаданных;
- AI для обнаружения утечек – предотвращение атак в реальном времени;
- гибкие настройки конфиденциальности – контроль над уровнями защиты.

PrivacyGuard – мессенджер нового поколения

Предлагаемая инновация – PrivacyGuard, мессенджер с акцентом на приватность. Его ключевые характеристики:

- полностью децентрализованная архитектура;
- сквозное шифрование с постквантовой защитой;
- минимальный сбор данных и защита от анализа метаданных;
- гибкие настройки для пользователей с разными уровнями риска;
- интеграция с блокчейном для аутентификации без номеров телефонов.

Конфиденциальность в мессенджерах – важная необходимость в цифровую эпоху. Даже при сквозном шифровании остаются уязвимыми метаданные. Безопасные мессенджеры часто неудобны, а популярные – недостаточно защищены. Решение – в новых технологиях: децентрализации, постквантовом шифровании, AI и блокчейне. Идея PrivacyGuard – шаг к балансу между безопасностью, удобством и свободой общения.

Список использованных источников:

1. Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ.
2. ГОСТ Р 59407-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных».
3. Ашманов И.С., Касперская Н.И. Цифровая гигиена. СПб.: Питер, 2021. 256 с.

4. Гуриков С.Р. Интернет-технологии: учебное пособие. М.: Форум: ИНФРА-М, 2019. 184 с.
5. Binance Academy. Что такое сквозное шифрование (E2EE)? URL: https://academy.binance.com/ru/articles/what-is-end-to-end-encryption-e2ee (дата обращения: 26.03.2025).
6. Anti-Malware.ru. Сравнительный анализ безопасности и приватности мессенджеров. URL: https://www.anti-malware.ru/compare/Messengers-security-and-privacy (дата обращения: 26.03.2025).
7. Blockchain-Enabled End-to-End Encryption for Instant Messaging Applications // arXiv. URL: https://arxiv.org/ abs/2104.08494 (дата обращения: 26.03.2025).
8. Сквозное шифрование: что это и почему это так важно? // SecurityLab.ru. URL: https://www.securitylab.ru/analytics/543882.php (дата обращения: 26.03.2025).
9. Практика применения постквантовых криптографических алгоритмов // Futurecrew.ru. URL: https://futurecrew.ru/blog/praktika-primeneniya-postkvantovyh-kriptograficheskih-algoritmov (дата обращения: 26.03.2025).

Taktaev T.U.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

PRIVACY IN MESSENGERS: HOW SECURE ARE OUR CHATS?

Abstract. The article discusses current privacy threats in messengers, protection methods including end-to-end and post-quantum encryption, and a concept of the next-generation messenger. Special attention is given to metadata protection and decentralization. The paper proposes ideas for developing a secure communication platform ensuring maximum confidentiality and user control.

Keywords: privacy, messengers, encryption, metadata, security.