

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ ШИФРОВАНИЯ В МЕССЕНДЖЕРАХ

В условиях современного мира вопрос безопасности мессенджеров становится все более важным. Какие мессенджеры предлагают лучшую защиту данных? Рассмотрим и оценим их на основе ключевых параметров безопасности. Signal использует технологию сквозного шифрования Double Ratchet, обеспечивая высокий уровень безопасности. Этот протокол предполагает использование временных ключей для каждого сообщения, обновление ключей после каждой передачи и поддержку прямой секретности (forward secrecy), что предотвращает компрометацию предыдущих или последующих ключей при взломе одного из них. Telegram в секретных чатах использует алгоритм Диффи-Хеллмана для создания общего секретного ключа без прямого обмена данными между пользователями. Это обеспечивает безопасность общения, поскольку ключи создаются и используются без возможности перехвата третьими лицами. Viber и WhatsApp также предлагают сквозное шифрование, но с некоторыми оговорками. Viber использует сквозное шифрование для всех сообщений, начиная с версии 6.0.0, и обеспечивает безопасность общения, хотя есть проблемы с хранением переписок только на устройстве пользователя. WhatsApp использует сквозное шифрование по умолчанию, но его резервные копии в облаке не зашифрованы, что создаёт потенциальные риски безопасности. В результате анализа выявлено, что мессенджеры Telegram, WhatsApp и Viber лидируют в рейтинге по уровню безопасности и приватности в Беларуси. Сравнивая мессенджеры, важно учитывать их преимущества и недостатки в контексте безопасности и приватности. Не существует абсолютно безопасного мессенджера, каждый из них имеет свои уникальные функции и потенциальные уязвимости. Выбор мессенджера зависит от индивидуальных потребностей пользователя и уровня безопасности.

Было уделено внимание функциям безопасности, которые предлагают различные мессенджеры, такие как биометрическая аутентификация, настройки приватности, которые позволяют пользователям более тонко настраивать уровень безопасности. Эти функции варьируются в зависимости от платформы, что влияет на общую оценку безопасности каждого мессенджера. Например, некоторые мессенджеры предлагают шифрование чатов и звонков по умолчанию, в то время как другие требуют от пользователя активировать эти функции в настройках.