УДК 004.056.5

Студ. К.А. Зыков
Науч. рук. доц., канд. техн. наук Н.И. Белодед
(кафедра программной инженерии, БГТУ)

МЕССЕНДЖЕР «CRYPTOGRAM»

В условиях стремительного развития цифровых технологий обеспечение безопасности общения становится особенно актуальным. Утечки персональных данных, взломы аккаунтов и атаки на популярные мессенджеры могут привести к серьезным последствиям - от кражи личной информации до мошенничества, шантажа и утечки корпоративных или государственных данных. Многие сервисы не обеспечивают должного уровня защиты, позволяя злоумышленникам перехватывать и использовать пользовательскую информацию. В этой ситуации пользователи всё чаще задумываются о способах защиты своей переписки и данных. Возникает потребность в инструментах, которые обеспечивают не просто удобство, но и надёжную конфиденциальность.

Cryptogram решает эту проблему с помощью клиентского шифрования, при котором шифровальные ключи создаются самими пользователями и хранятся исключительно на их устройствах, не передаваясь ни на сервер, ни в облако. Это означает, что даже при компрометации сервера или взломе аккаунта третьи лица не смогут получить доступ к переписке или отправлять сообщения от имени пользователя. Благодаря такому подходу, Cryptogram полностью исключает возможность вмешательства извне. Все сообщения шифруются на устройстве отправителя до отправки и расшифровываются только на устройстве получателя – сервер в этом процессе выступает лишь как передатчик зашифрованных данных и не имеет доступа к их содержимому.

Основная цель разработки Cryptogram - создать мессенджер, в котором безопасность реализована через полную автономию пользователя: он сам задает ключ, который должен быть известен собеседнику, а при утрате ключа доступ к сообщениям становится невозможным. Такая модель исключает возможность восстановления ключа, но гарантирует, что данные останутся недоступными посторонним.

В основе системы лежит метод шифрования, вдохновлённый шифром Вернама: сообщение и ключ переводятся в битовое представление, после чего применяется операция XOR. Ключ состоит из 16-значного числа, что дает 10 квадриллионов возможных комбинаций - взлом такого шифра потребует десятки лет даже при использовании мощных вычислительных ресурсов.

Cryptogram эффективно противостоит распространённым угрозам