

УДК 004
БК 32.973.202

Матеріали X-ої Ювілейної Міжнародної науково-практичної конференції «Free and Open Source Software». Харків, 20-22 листопада 2018 р. – Харків: Харківський національний університет будівництва та архітектури, 2018. – 121 с.

Представлено матеріали пленарних та секційних засідань X-ої Ювілейної Міжнародної науково-практичної конференції «Free and Open Source Software». Обговорено основні проблеми, науково-технічні досягнення, впровадження і досвід використання сучасних технологій в області безкоштовних програмних продуктів, а також з відкритим вихідним кодом. Висвітлено основні питання безкоштовного прикладного, серверного програмного забезпечення та прикладного програмного забезпечення з відкритим вихідним кодом, безкоштовних сервісів, а також ліцензування та правових аспектів використання безкоштовного програмного забезпечення Для фахівців науково-дослідних, комерційних організацій, аспірантів та студентів

Редакційна колегія:
Старкова О.В. – голова, доц., д.т.н.;
Міхеев І.А. – к.т.н.;

Відповідальний за випуск:
д.т.н., доц. Старкова О.В.

Роботи надруковані з авторських оригіналів, що надані оргкомітету, за авторської редакції.

Електронний варіант матеріалів конференції доступний на сайті кафедри ЕКІТ ХНУБА:

<http://kn-it.info/>

та на сайті конференції:

<http://foss.kn-it.info/>

ОСОБЛИВОСТІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В TELEGRAM

Збаражський К.А., Давидова В.П.

Керівник: Шеховцова В.І.

E-mail: kyrylo.zbarazhskiy@nure.ua, veronika.davydova@nure.ua

Харків. Харківський національний університет радіоелектроніки

Постановка проблеми. Telegram – безкоштовний багатофункціональний месенджер, що дозволяє обмінюватися повідомленнями і медіафайлами різних форматів. Зробивши порівняльний аналіз Telegram та інших месенджерів ми виділили такі його переваги:

- трафік нікому не вдалося розшифрувати;
- відкритий код;
- відсутня реклама;
- сервери знаходяться в 5 різних точках світу;
- до 200 учасників в одній бесіді.

Telegram використовує, спеціально створений для додатка, протокол зв'язку MTProto. У месенджері є хмарні і секретні чати. В останніх використовується шифрування end-to-end, тобто повідомлення шифрується на телефоні відправника, а розшифровується тільки у одержувача. Решта чатів, у тому числі приватні повідомлення, канали і групи – хмарні, вони шифруються на телефоні, передаються за допомогою протоколу MTProto на сервери месенджера, там розшифровуються і зберігаються.

Proto – криптографічний протокол, який використовується в системі обміну повідомленнями Telegram для шифрування листування користувачів. Він працює на основі наступних алгоритмів:

- AES – симетричний 256-бітний алгоритм, прийнятий урядом США як стандарт;
- RSA – криптографічний алгоритм, в основі якого лежить обчислювальна складність завдання факторизації великих цілих чисел;
- Метод Діффі-Хеллмана – дозволяє отримати двом і більш співрозмовникам секретний ключ по незахищеному від прослуховування, однак захищеному від підміни каналу зв'язку;
- SHA-1, MD5 – хеш-алгоритми, використовуються в багатьох криптографічних протоколах і додатках для безпечного хешування.

Висновок. Ступінь захищеності даних в Telegram, є одним з кращих. Тому даний месенджер – це найкраще рішення для захисту ваших даних і листування.

Література

- [1] Telegram // Вікіпедія. [Електронний ресурс]. – Режим доступу до ресурсу: <https://ru.wikipedia.org/wiki/Telegram>
- [2] Рябухіна Ю. Telegram. Что это такое и почему это круто //Keddr.com. [Електронний ресурс]. – Режим доступу до ресурсу: <https://keddr.com/2014/11/telegram-cto-to-takoe-i-pochemu-eto-kruto/>