

UDC 004

TELEGRAM IN THE FIELD OF PRODUCTION AND STUDY*Kis I. S., Skrypnyk N.S.**Kharkiv National Automobile and Highway University, Kharkiv*

Telegram is a freeware, cross-platform, cloud-based instant messaging (IM) software and application service. The service also provides end-to-end encrypted video calling, file sharing and several other features.

Telegram provides end-to-end encrypted voice and video calls and optional end-to-end encrypted "secret" chats. Cloud chats and groups are encrypted between the app and the server, so that ISPs and other third-parties on the network can't access data, but the Telegram server can. Users can send text and voice messages, animated stickers, make voice and video calls, and share an unlimited number of images, documents (2 GB per file), user locations, contacts, and audio files. In January 2021, Telegram surpassed 500 million monthly active users. It was the most downloaded app worldwide in January 2021.

Study: Telegram is used in many Ukrainian universities. Telegram helps teachers get and keep in touch with their students. It also helps students to communicate with each other.

Production: Telegram is used for communication of workers and management. This is especially true at the present time, because of the Coronavirus, most people work from home, for comfortable communication, in most cases, people use Telegram. Messages can also be sent with client-to-client encryption in so-called *secret chats*. These messages are encrypted with the service's MTProto protocol.[67] Unlike Telegram's cloud-based messages, messages sent within a secret chat can be accessed only on the device upon which the secret chat was initiated and the device upon which the secret chat was accepted; they cannot be accessed on other devices. Messages sent within secret chats can, in principle, be deleted at any time and can optionally self-destruct. Secret chats have to be initiated and accepted by an invitation, upon which the encryption keys for the session are exchanged. Users in a

secret chat can verify that no man-in-the-middle attack has occurred by comparing pictures that visualize their public key fingerprints. According to Telegram, secret chats have supported perfect forward secrecy since December 2014. Encryption keys are periodically changed after a key has been used more than 100 times or has been in use for more than a week. Old encryption keys are destroyed. Windows and Linux users are still not able to use secret chats using the official Telegram Desktop app while the official macOS-only client supports them. Secret chats are not available for groups or channels.

Secret chats help to make some business decisions, in secret from competitors

At the end of March 2017, Telegram introduced its own *voice calls*. The calls are built upon the end-to-end encryption. Connection is established as peer-to-peer whenever possible; otherwise the closest server to the client is used. According to Telegram, there is a neural network working to learn various technical parameters about a call to provide better quality of the service for future uses. After a brief initial trial in Western Europe, *voice calls* are now available for use in most countries.

Telegram announced in April 2020 that they would include *group video calls* by the end of the year. On 15 August 2020, Telegram added video calling with end-to-end encryption like Signal and WhatsApp, which Zoom does not have yet. Currently offering one-to-one video calls, Telegram has plans to introduce secure group video calls later. Picture-in-picture mode is also available so that users have the option to simultaneously use the other functions of the app while still remaining on the call and are even able to turn their video off. Telegram's video and voice calls are secure and end-to-end encrypted

References:

1. Rosenberg A. История создания Telegram. (2017) URL: <https://medium.com/@anton.rozenberg/telegram-telegraph-durov-short-history-750a26f9cb42>
2. История Telegram: от идеи до собственной криптовалюты (2020). URL: <https://habr.com/ru/post/489252/>
3. Telegram URL: <https://uk.wikipedia.org/wiki/Telegram>