

**Голікова Олена Валеріївна,**

*завідувач сектору авторського права та суміжних прав лабораторії авторського права та інформаційних технологій, Науково-дослідний центр судової експертизи з питань інтелектуальної власності, бульвар Л. Українки, 26, офіс 501, м. Київ, 01133, e-mail: ov\_golikova@ukr.net, тел.: +38 044 5921401, <https://orcid.org/0000-0002-2487-3637>*

**Заїкіна Тетяна Василівна,**

*судовий експерт сектору інформаційних технологій лабораторії авторського права та інформаційних технологій, Науково-дослідний центр судових експертиз з питань інтелектуальної власності, бульвар Л. Українки, 26, офіс 501, м. Київ, 01133, тел.: +38 044 5921401, e-mail: zaikina.tv@ukr.net, <https://orcid.org/0000-0002-3839-5859>*

## **ОСОБЛИВОСТІ ДОСЛІДЖЕННЯ СИСТЕМ ОБМІНУ МИТТЄВИМИ ПОВІДОМЛЕННЯМИ (МЕСЕНДЖЕРУ) «TELEGRAM»**

**Анотація.** На сьогоднішній день в Україні відсутні єдині методичні підходи проведення судових експертиз та експертних досліджень у частині що стосується вилучення та аналізу мультимедійних даних із терміналів мобільного зв'язку, зокрема вмісту мобільного застосунку/месенджера Telegram.

Це призводить до використання у державних спеціалізованих експертних установах різних підходів, методик та алгоритмів, що в окремих випадках суперечать між собою, обумовлює необхідність призначення повторних судових експертиз.

Telegram – це багатоплатформовий клауд-месенджер (хмарний месенджер) з функціями VoIP для смартфонів, планшетів та ПК, який дозволяє обмінюватися текстовими, голосовими та відеоповідомленнями, стікерами та фотографіями, файлами багатьох форматів. Можна також здійснювати відео- і аудіодзвінки, організувати відеоконференції, розраховані на групи і канали з багатьма користувачами. Клієнтські програми Telegram доступні для Android, iOS, Windows Phone, Windows, macOS і GNU/Linux.

Окрім обміну повідомленнями в діалогах і групах, в месенджері можна зберігати необмежену кількість файлів, вести канали (мікроблоги), створювати і використовувати ботів.

Telegram передбачає безперервну синхронізацію і, як результат, можливість отримання доступу до своїх повідомлень одночасно з кількох пристроїв, включаючи планшети та комп'ютери, а також надавати необмежену кількість фотографій, відео та файлів (doc, zip, mp3 тощо) обсягом до 2 ГБ кожен.

Telegram зберігає лише інформацію, необхідну для функціонування як багатофункціональний хмарний сервіс. Наприклад, хмарні чати з метою отримання доступу з будь-яких пристроїв, не використовуючи сторонні резервні копії або свої контакти.

Telegram використовується на декількох платформах із безперервною синхронізацією. Однак, можливі випадки, коли повідомлення, розміщене на одній платформі, не відображається на іншій та з'являється без відома кінцевого користувача.

Можливість виникнення таких випадків та їх подальше дослідження і розглядається у даній статті.

**Ключові слова:** системи обміну миттєвими повідомленнями, месенджери, дослідження програмних продуктів, Android, iOS, Telegram.

**Holikova Olena Valerievna,**

*Head of the copyright and related rights copyright and related rights laboratory of the Copyright and Information Technologies Laboratory, Research Center for Forensic Expertise on Intellectual Property, 26, L. Ukrainka Boulevard, office 501, Kyiv, 01133, e-mail: ov\_golikova@ukr.net; +38 044 5921401, <https://orcid.org/0000-0002-2487-3637>*

**Zaikina Tetyana Vasylivna,**

*Forensic Expert of the Information Technology Sector of the Laboratory of Copyright and Information Technologies, Research Center for Forensic Intelligence on Intellectual Property, 26 L. Ukrainka Boulevard, Office 501, Kyiv, 01133, tel .: +38 044 5921401 , e-mail: zaikina.tv@ukr.netb [https // orcid.org / 0000-0002-3839-5859](https://orcid.org/0000-0002-3839-5859)*

## **FEATURES OF RESEARCH OF INSTANT MESSAGE EXCHANGE SYSTEMS (MESSENGER) «TELEGRAM»**

**Abstract.** Now, Ukraine does not have uniform methodological approaches to conducting forensic examinations and expert research in the area of extraction and analysis of multimedia data from mobile terminals, in particular the content of the mobile application / messenger Telegram.

This leads to the use of different approaches, methods and algorithms in state specialized expert institutions, which in some cases contradict each other, necessitates the appointment of repeated forensic examinations.

Telegram is a multi-platform cloud messenger (cloud messenger) with VoIP features for smartphones, tablets and PCs, which allows you to exchange text, voice and video messages, stickers and photos, files in many formats. You can also make video and audio calls, organize video conferences for groups and channels with many users. Telegram clients are available for Android, iOS, Windows Phone, Windows, macOS and GNU / Linux.

In addition to exchanging messages in dialogs and groups, you can store an unlimited number of files in the messenger, maintain channels (microblogs), create and use bots.

Telegram provides seamless synchronization and, as a result, the ability to access your messages simultaneously from multiple devices, including tablets and computers, as well as provide an unlimited number of photos, videos and files (doc, zip, mp3, etc.) up to 2 GB each .

Telegram stores only the information necessary to function as a multifunctional cloud service. For example, cloud chats to access from any device without using third-party backups or your contacts.

Telegram is used on several platforms with continuous synchronization. However, there may be cases where a message placed on one platform does not appear on another and appears without the end user's knowledge. The possibility of such cases and their further study is considered in this article.

**Keywords:** instant messaging systems, messengers, software research, Android, iOS, Telegram.

**Постановка проблеми.** На сьогоднішній день відсутні єдині підходи для аналізу сервісів миттєвого обміну повідомлення, зокрема такого сервісу як Telegram. З метою аналізу можливостей такого сервісу, а також з метою визначення можливості створення «фейкових» повідомлень та подальшого їх аналізу проведено дане дослідження.

**Аналіз останніх досліджень і публікацій.** Наукові дослідження щодо особливостей дослідження систем миттєвого обміну повідомленнями, зокрема месенджеру Telegram не знайдено.

**Метою роботи** є опис проблемних питань у процесі визначення/встановлення можливості направлення «фейкових» повідомлень за допомогою засобу передачі повідомлень (месенджеру) на прикладі месенджеру Telegram.

**Виклад основного матеріалу.** За результатами наявного досвіду та визначеної задачі, питанням, що вирішувалось під час аналізу сервісу обміну миттєвими повідомленнями було визначено наступне: *Чи можливе відправлення повідомлень у системі обміну миттєвими повідомленнями, а саме хмарному месенджері для мобільних пристроїв та комп'ютерів «Telegram», у тому числі медіаповідомлень від імені власника облікового запису сторонніми особами (без дозволу власника відповідного облікового запису)? Якщо так, то яким чином і за яких умов?*

При проведенні експертизи відповідно до вимог Інструкції та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень використовуються методи дослідження: аналіз, синтез, конкретизація, аналогія, порівняння з ураху-

ванням методологічних основ судової експертизи, методичних рекомендацій та рекомендованої літератури, відповідних затверджених методик та методичних рекомендацій.

Об'єктами дослідження у даних дослідженнях є мобільні телефони.

Дослідження питань здійснюється із застосуванням спеціалізованих засобів – автоматизованого робочого місця експерта на основі спеціалізованого програмного забезпечення.

Щодо сервісу обміну миттєвими повідомленнями Telegram слід зазначити наступне.

Telegram – це багатоплатформовий клауд-месенджер (хмарний месенджер) з функціями VoIP для смартфонів, планшетів та ПК, який дозволяє обмінюватися текстовими, голосовими та відеоповідомленнями, стікерами та фотографіями, файлами багатьох форматів. Можна також здійснювати відео- і аудіодзвінки, організувати відеоконференції, розраховані на групи і канали з багатьма користувачами. Клієнтські програми Telegram доступні для Android, iOS, Windows Phone, Windows, macOS і GNU/Linux.

Telegram for Desktop це застосунок для ЕОМ на базі операційних систем Windows, macOS та Linux який надає можливість безпосередньо за допомогою ЕОМ використовувати сервіс обміну миттєвими повідомленнями.

У процесі дослідження аналізувались загальні характеристики та функціональні можливості програмного застосунку Telegram (версія Desktop Windows). За результатами проведеного дослідження було встановлено наступне.

Після встановлення програмного забезпечення на ЕОМ, з метою його

безперешкодного використання, необхідно авторизуватись у програмному забезпеченні **Telegram Desktop** за допомогою мобільного телефону. Процедура авторизації можливо пройти або скануванням QR-коду, що генерується у **Telegram Desktop**, або вводу коду, що може бути надісланий на номер телефону з якого виконується авторизація.

Додатково варто зазначити, що при спробі підтвердження входу до Telegram Desktop з використанням сканування QR-коду, який було запропоновано відсканувати за допомогою клієнтського застосунку на мобільному пристрої, реєстрація відбувається успішно навіть з вилученою SIM-картою. Внаслідок реєстрації відбувається під'єднання застосунку до мережі, а абоненту до службового чату було направлено повідомлення про подію на мобільний пристрій та повідомлення з паролем на ЕОМ. Таким чином, **існує можливість отримання доступу до застосунку Telegram Desktop з використанням мобільного телефону із встановленим застосунком Telegram, навіть у випадку вилучення з телефону SIM-картки.**

Окремо варто зазначити, що серед іншого, Telegram передбачає так звану двофакторну ідентифікацію, але на відміну від більшості сервісів СМС у схемі автентифікації користувача є головним фактором, а пароль – додатковим. За замовчуванням такий спосіб у Telegram не використовується, зайвих нагадувань про таку можливість користувач не отримує.

Після успішної авторизації користувача у Telegram Desktop за допомогою мобільного пристрою, наявні та відображені на мобільному пристрої бесіди/чати (медіаповідомлення) син-

хронізуються (за виключенням закритих (секретних) бесід) та відображаються у програмному забезпеченні Telegram Desktop.

*Довідково. Секретні чати, функціональність застосунку призначена для забезпечення користувачів більшою конфедіційністю, ніж звичайні чати. Всі повідомлення в секретних чатах використовують наскрізне шифрування, наслідком чого є те, що тільки відправник та одержувач даних можуть читати ці повідомлення. Крім того, на повідомлення в секретних чатах діє заборона застосунку на пересилання, копіювання та зняття скріншоту. У разі видалення повідомлення його відправником, на своєму пристрої, застосунок на іншій стороні секретного чату також отримує директиву/команду на видалення контенту у повному обсязі. Також у таємному чаті наявний функціонал щодо самознищення даних за таймером – через певний проміжок часу, після того, як повідомлення/контент прочитані або відкриті одержувачем. Знищення повідомлення відбувається на усіх пристроях на яких відбувався чат.*

Окрім того, була розглянута можливість віддаленого підключення до комп'ютера зі встановленим програмним забезпеченням Telegram Desktop та/або веб-версії Telegram Web. На сьогоднішній момент існує декілька способів віддаленого підключення та керування комп'ютером таких як:

- Підключення до віддаленого робочого столу по RDP-протоколу засобами операційної системи;
- підключення до комп'ютера користувача використовуючи стороннє програмне забезпечення (TeamViewer, AnyDesk, Ammyu Admin тощо). Вищезазначені програмні продукти нада-

ють доступ до віддаленого керування по ID комп'ютеру та паролі, які генеруються на комп'ютері над яким необхідно отримати керування. Для встановлення зв'язку вищезазначені програмні продукти повинні бути запущені на обох машинах. Щоб встановити зв'язок між комп'ютерами, клієнт-оператор повинен зв'язатися з віддаленим оператором і дізнатися його ID і пароль, а потім ввести їх в клієнт даного програмного забезпечення;

- віддалене керування по протоколу telnet;

- інфікування комп'ютера до якого необхідно отримати доступ за допомогою шкідливого програмного забезпечення (TeamSpy, троянські програми, Remote Access Trojan (троянські програми віддаленого доступу) тощо). В даному випадку користувач не обізнаний про те, що до його комп'ютера мається віддалений доступ у сторонніх осіб.

Довідково:

*Троянська програма – різновид шкідливої програми, яка проникає в комп'ютер під виглядом легального програмного забезпечення. Основні функції:*

- закачування і викачування файлів;
- копіювання помилкових посилань, що ведуть на підроблені веб-сайти, чати або інші сайти з реєстрацією;

- створення перешкод роботі користувача;

- крадіжка даних, що представляють цінність або таємницю, в тому числі інформації для автентифікації, для несанкціонованого доступу до ресурсів, видобування деталей щодо банківських рахунків, які можуть бути використані в злочинних цілях;

- поширення інших шкідливих програм, таких як віруси;

- знищення даних (стирання або переписування даних на диску) і обладнання, виведення з ладу або відмови обслуговування комп'ютерних систем, мереж;

- збір адрес електронної пошти і використання їх для розсилки спаму;

- стеження за користувачем і таємне повідомлення третім особам відомостей, таких як, наприклад, звичка відвідувати конкретні сайти;

- реєстрація натискань клавіш з метою крадіжки інформації такого роду як паролі та номери кредитних карток;

- дезактивація або створення перешкод роботі антивірусних програм і брандмауера.

При отриманні одним з вищенаведених способів, віддаленого доступу до комп'ютера зі встановленим програмним забезпеченням Telegram Desktop та/або з відкритим у веб-браузері Telegram Web у сторонньої особи з'являється можливість відправляти повідомлення у системі обміну миттєвими повідомленнями Telegram, зокрема відправлення медіаповідомлень від імені власника облікового запису.

Також варто зазначити, що застосунок Telegram Desktop, встановлений на ЕОМ користувача, не має жодних додаткових способів захисту, а також постійно знаходиться у фоновому режимі (у випадку, якщо користувач самостійно не здійснить вихід із застосунку). Таким чином, у **випадку несанкціонованого доступу до ЕОМ засобами, що дозволяють віддалене керування комп'ютером, існує можливість несанкціонованого доступу**



## **і до застосунку Telegram Desktop без будь-яких додаткових дій.**

Окрім того, у процесі дослідження виявлено можливість використання застосунку *Telegram* за допомогою веб-браузера.

Програмне забезпечення *Telegram Web* призначене для доступу до системи обміну повідомленнями *Telegram* за допомогою веб-браузерів (*Google Chrome*, *Mozilla Firefox*, *Edge* тощо).

Експертами, використовуючи веб-браузер **Google Chrome** було виконано перехід за посиланням <https://web.telegram.org/> та виконано вхід до веб-версії програмного застосунку «**Telegram Web**». Вхід виконується за допомогою сканування QR-коду мобільним телефоном.

Окремо варто зазначити, що для отримання коду з підтвердженням входу до програмного забезпечення *Telegram Desktop/Telegram Web* відсутня необхідність у розблокуванні мобільного телефону, так як повідомлення з кодом відображається у вигляді спливаючого сповіщення на екрані заблокованого мобільного телефону, **що дає можливість стороннім особам без відома кінцевого користувача отримати зазначений код та в подальшому здійснити авторизацію з можливістю доступу до вмісту електронного листування та подальшого його вивантаження.**

Окремо слід зауважити, що при отриманні будь-якого повідомлення (в тому числі і в телеграм-каналах) чат в який було направлено повідомлення буде відображатися першим (зверху). В даному випадку присутній «людський фактор», користувач може не звернути увагу на те, що в якомусь чаті з'явилися повідомлення, котрі

він не відправляв (вони були зроблені з іншого пристрою), внаслідок чого користувач фактично не є проінформований про наявність такого інформаційного трафіку.

## ***Щодо принципу обміну повідомленнями за допомогою месенджера Telegram:***

*Telegram* є месенджером з «безшовною синхронізацією», тобто таким, який орієнтований на одночасне використання на кількох пристроях, зазвичай, але не виключно різних форм-факторів. Тобто, месенджер конструктивно призначений для під'єднання кількох пристроїв до єдиного облікового запису. Передбачені виробником можливості дозволяють:

- під'єднати для облікового запису спеціальний програмний засіб для персонального комп'ютера, внаслідок чого користувач облікового запису отримує можливість брати участь у обмінні повідомленнями мережею *Telegram*, використовуючи в якості терміналу персональний комп'ютер;
- під'єднати до облікового запису додатковий портативний пристрій, який буде використовуватись для обміну повідомленнями мережею *Telegram*.

Основним місцем зберігання листувань є **хмарне сховище системи**, з якого під'єднані до облікового запису пристрої отримують повідомлення та медіаматеріали.

Стосовно програмних засобів, які дають можливість користуватись системою обміну повідомленнями *Telegram*, слід зазначити наступне:

- в номенклатурі наявні програмні засоби для більшості мобільних плат-

форм, включаючи різноманітні версії Android та iOS;

- в номенклатурі наявні програмні засоби для персональних комп'ютерів під керуванням: Windows (звичайний клієнт, який зберігає параметри налаштування у системному реєстрі, та портативний клієнт — варіант програмного засобу, який зберігає параметри налаштування у файлах в своїй теці), Linux та macOS.

Листування у системі Telegram зберігаються у власному хмарному сервісі системи, що принципово обумовлює можливість доступу з кількох абонентських пристроїв. Відповідно, бази даних не входять до складу резервних копій систем. Тобто, у локальних сховищах пристроїв не зберігаються бази даних повідомлень, але кешовані дані все ж присутні у системі.

Telegram зберігає повну історію листування користувачів на власних серверах — за винятком секретних чатів.

Окрім того, за результатами аналізу функціональних можливостей програмного забезпечення **Telegram Desktop** виявлено можливість експортувати всі дані, що зберігає Telegram на сервері.

Згідно з правилами GDPR, користувач повинен мати доступ до зібраної про себе інформації. Тому, за допомогою цієї функції існує можливість отримати копію своїх даних, які зберігає Telegram.

Довідково:

**Загальний регламент про захист даних** (англ. **General Data Protection Regulation, GDPR; Regulation (EU) 2016/679**) — регламент в межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Вона також

*стосується експорту персональних даних за межі ЄС і ЄЕЗ. GDPR покликаний насамперед надати громадянам та резидентам ЄС контроль за їхніми персональними даними та спростити регуляторне середовище для міжнародного бізнесу шляхом уніфікації регулювання в межах ЄС.*

Експортування даних відбувається за наступним алгоритмом:

«Настройки => Продвинутые настройки => Экспорт данных из Telegram»

В подальшому користувачеві пропонується обрати зі списку дані, копію яких необхідно отримати. Можливо вивантажити контакти, особисті чати, чати в групах і ботах, мультимедійні дані: фото, відео, аудіо, документи і т.д, загалом все, що зберігається на серверах месенджера. Вивантажити дані можна в двох форматах — HTML або JSON.

На інші пристрої, в цілях безпеки, надходить повідомлення про запит на експорт даних. Щоб переконатися в тому, що запит відправлено дійсно особою, що звертається для експорту даних і, в разі чого, користувач мав змогу відреагувати, завантаження можливо розпочати тільки через 24 години.

Окрім того, варто зазначити, що Telegram не використовує ніякого додаткової захисту. Для доступу до даних досить образу файлової системи. Таким чином, у випадку створення образу файлової системи із заздалегідь встановленим та активованим застосунком Telegram, та подальшим його розгортанням (відновленням) на автоматизованому робочому місці (APM/EOM), застосунок буде віднов-

лено у повному обсязі із збереженням повного доступу до нього.

*Алгоритм дослідження системи миттєвого обміну повідомленнями, зокрема месенджеру Telegram (експертний експеримент):*

Для підтвердження функціональних можливостей додатку Telegram було визначено алгоритм проведення експертного експерименту:

1. Завантаження програмного застосунку «Telegram» з App Store, первинна реєстрація, створення облікового запису «Експерт Тест».

2. Тестова передача повідомлень (медіа повідомлень – текстових, графічних, гіперпосилань, звукових) у програмному застосунку «Telegram» між абонентами «Експерт Тест» та «ARM\_Expert».

3. Інсталяція Telegram Desktop, версії 2.8.1 на АРМ експерта. Отримання коду для входу у Desktop версію Telegram на мобільний пристрій (варіанти входу та отримання коду).

4. Тестова передача повідомлень (медіа повідомлень: текстових, графічних, гіперпосилань, звукових) у програмному застосунку «Telegram Desktop» між абонентами «ARM\_Expert» та «Експерт Тест» (підтвердження синхронізації відкритих чатів).

5. Тестова передача повідомлень (медіа повідомлень: текстових, графічних, гіперпосилань, звукових) у програмному застосунку «Telegram Desktop» між абонентами «ARM\_Expert» та «Експерт Тест» з використанням «секретного чату». Підтвердження відсутності синхронізації такого чату з Telegram Desktop.

6. Перехід за посиланням <https://web.telegram.org/> з використанням веб-браузера Google Chrome та авто-

ризація до веб-версії програмного застосунку «Telegram Web».

7. Тестова передача повідомлень у веб-версії програмного застосунку «Telegram Web» та під'єднання до телеграм-каналів.

**Висновки.** Таким чином за результатом проведення аналізу та повного дослідження із проведенням експертних експериментів, визначено, що відправлення повідомлень у системі обміну миттєвими повідомленнями Telegram, зокрема відправлення медіаповідомлень від імені власника облікового запису сторонніми особами (без дозволу власника відповідного облікового запису) можливе.

Для відправлень повідомлень від імені власника облікового запису сторонніми особами (без дозволу власника відповідного облікового запису) можливо за умови здійснення авторизації в одному з зазначених програмних продуктів – Telegram, Telegram Desktop, Telegram Web. Для цього необхідне виконання умов:

- отримати фізичний доступ до розблокованого мобільного телефону на якому міститься програмне забезпечення Telegram та авторизуватись за допомогою цього телефону в програмному забезпеченні Telegram Desktop або Telegram Web;

- отримати фізичний доступ до заблокованого мобільного телефону на якому міститься програмне забезпечення Telegram, з метою отримання коду підтвердження авторизації (повідомлення з кодом відображається сповіщенням на заблокованому мобільному телефоні) в програмному забезпеченні Telegram Desktop або Telegram Web;



- отримати фізичний доступ до SIM-карти мобільного телефону, на якому міститься програмне забезпечення Telegram з метою подальшого клонування зазначеної SIM-карти та отримання доступу до телекомунікаційної мережі з подальшим отриманням коду підтвердження для входу в програмне забезпечення Telegram;

- отримати віддалений доступ до комп'ютера з інсталюваним програмним забезпеченням Telegram Desktop та/або з відкритим у веб-браузері Telegram Web.

Після зазначених дій стороння особа отримує доступ до програмного забезпечення Telegram, що дає змогу відправляти повідомлення та переглядати чати з електронним листуванням. Також за допомогою програмного забезпечення Telegram Desktop можливо провести експортування усіх даних (контакти, чати з повідомленнями, медіаповідомлення, електронні документи тощо), що зберігаються на сервері Telegram щодо відповідного користувача.

## **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**

---

1. Великий тлумачний словник сучасної української мови / уклад. та голов. ред. В. Т. Бусел. Київ, 2005. 1728 с.

2. Методика № 10.9.07 «Дослідження інформації на цифрових носіях» Реєстр методик проведення судових експертиз. URL: <http://rmpse.minjust.gov.ua/search> (дата звернення: 22.10.2020).

3. Тлумачний словник з інформатики / Г.Г. Півняк, Б.С. Бусигін, М.М. Дівізійнюк та ін. Д., Нац. Гірнич. ун-т, 2010. 600 с.

4. Telegram (офіційний веб-сайт застосунку) URL: <https://telegram.org/> (дата звернення: 10.12.2021)

## **REFERENCES:**

---

1. Busel, V. T. (Eds.). (2005). Velykyi tлумachnyi slovnyk suchasnoi ukrainiskoi movy [Large explanatory dictionary of the modern Ukrainian language]. Kyiv [in Ukrainian].

2. Metodyka № 10.9.07 «Doslidzhennia informatsii na tsyfrovyykh nosiiakh» [Research of information on digital media]. Reiestr metodyk provedennia sudovykh ekspertyz. <http://rmpse.minjust.gov.ua/search> Retrieved from <http://rmpse.minjust.gov.ua/search>.

3. Pivniak, H.H., Busyhin, B.S., Diviziniuk, M.M. (2010). Tlumachnyi slovnyk z informatyky [Explanatory dictionary of computer science]. Donetsk [in Ukrainian].

4. Telegram (official web-site of application) <https://telegram.org/> Retrieved from <https://telegram.org/> [in Ukrainian]