

Юридичні науки

УДК 004.4.7

Глотов Олександр Миколайович

старший судовий експерт

Харківський науково-дослідний експертно-криміналістичний центр МВС

Glotov Oleksandr

Senior Forensic Expert

Kharkiv Scientific Research Forensic Center of the Ministry of Internal Affairs

**ОСОБЛИВОСТІ ДОСЛІДЖЕННЯ МОБІЛЬНИХ МЕСЕНДЖЕРІВ
ТА ВИЛУЧЕННЯ ДАНИХ ПРИ ВИРІШЕННІ КРИМІНАЛЬНИХ
РОЗСЛІДУВАНЬ**

**FEATURES OF MOBILE MESSENGER RESEARCH AND DATA
EXTRACTION IN SOLVING CRIMINAL INVESTIGATIONS**

***Анотація.** Вступ. Інтернет набуває популярності, тому відбуваються зміни кожного року, 4G замінює 5G та займає не останнє місце в житті звичайних користувачів. Майже більшість користувачів Інтернету мають сучасні смартфони та айфони, використовують Інтернет для додатків, щоб знаходитися постійно на зв'язку та онлайн. Безліч додатків дозволяють спілкуватися вільно, мобільно та безпечно. Ця форма спілкування є не тільки популярною для досліджень, а також є необхідною для вживання в професійній діяльності спеціалістів певного профілю.*

У статті висвітлено проблему визначення поняття месенджери, їх різновид та вживаність у повсякденному житті звичайних користувачів різного віку. Виділено низку методів вилучення даних, необхідних для розслідування справ, які були видалені з додатків телефонів юзерів,

здатність безпечно використовувати мобільні пристрої, додатки та програми як у професійній діяльності, так і у загальному вжитку. Показано, що до цифрової бази даних належить передача звукової, текстової інформації, одержання зображень. Розглянуті такі популярні месенджери, як Viber, Facebook Messenger, Skype, Телеграм, Signal.. У статті вживається інформація, щодо використання популярних додатків різними віковими категоріями користувачів. Переваги та недоліки окремих месенджерів, та безпечність користування ними.

Висвітлені дослідження програмного забезпечення при вирішенні питань різного виду розслідувань.

Мета. Виділити основні методи вилучення отриманих необхідних даних з додатків мобільних пристроїв. Визначити найбільш ефективні методи для використання спеціалістами у професійній діяльності.

Матеріали і методи. Основним методом став системний підхід до отримання даних, який показує комунікацію в Інтернеті як інформаційну культуру суспільства. Порівняльний метод дає змогу виявити недоліки та переваги різних додатків.

Результати. Результатами нашого дослідження є виявлення комунікації в месенджерах, безпечне використання додатків мобільних пристроїв для користувачів різних вікових категорій.

Перспективи. Подальше дослідження месенджерів, для виявлення даних у професійній сфері спеціалістів, пошук методів дослідження та відслідковування нових месенджерів, що з'являються.

Ключові слова: месенджери, дані, мобільні застосунки, Інтернет.

Summary. Introduction. The Internet is gaining popularity, so changes occur every year, 4G replaces 5G and occupies not the last place in the lives of ordinary users. Almost the majority of Internet users have modern smartphones and iPhones, use the Internet for applications to be constantly connected and

online. Many applications allow you to communicate freely, mobilely and safely. This form of communication is not only popular for research, but also necessary for using in the professional activities of specialists of a certain profile.

The article highlights the problem of defining the concept of messengers, their types and use in the every day life of ordinary users of different ages. A number of methods for extracting data are necessary for investigating cases that were deleted from user phone applications, the ability to safely use mobile devices, applications and programs both in professional activities and in general use are highlighted. It is shown that the digital database includes the transmission of sound, text information, and receiving images. Such popular messengers as Viber, Facebook Messenger, Skype, Telegram, Signal are considered. The article uses information on the use of popular applications by different age categories of users. Advantages and disadvantages of individual messengers, and the safety of using them.

Software research is highlighted in solving issues of various types of investigations.

Purpose. To highlight the main methods of extracting the necessary data from mobile device applications. To determine the most effective methods for use by specialists in professional activities.

Materials and methods. The main method was a systematic approach to obtaining data, which shows communication on the Internet as the information culture of society. The comparative method allows you to identify the shortcomings and advantages of different applications.

Results. The results of our study are the detection of communication in messengers, the safe use of mobile device applications for users of different age categories.

Prospects. Further research on messengers to detect data in the professional field of specialists, the search for research methods and tracking new messengers that appear.

Key words: *messengers, data, mobile applications, Internet.*

Постановка проблеми. Сучасне суспільство не уявляє повсякденне життя без мобільних телефонів, Інтернету та різних додатків для спілкування. В умовах сьогодення спілкування, за допомогою месенджерів набуло великої популярності. Це відноситься до різних вікових груп та верств населення. Використання месенджерів набуває популярності у багатьох сферах життя.

Згідно опитування Київського міжнародного інституту соціології найбільш популярними додатками, якими користуються українці є Viber, Facebook Messenger, Skype, Телеграм, Signal. Соціальні мережі використовуються для поширення інформації та стають популярними, бо мають багато переваг, користувачі можуть обирати час та місце використання додатків.

Дослідженням месенджерів як засобу спілкування займалися багато науковців, серед них Н. Дькопулос, А. Бобков, С. Маєрс. Кожен з них наголошує, що месенджери є популярним способом спілкування, поширення інформації та також вилучення необхідної інформації для спеціальних служб.

Метою є довести наскільки та які месенджери загальноновживані, їх місце у використанні для листування та спілкування між певними категоріями людей.

Аналіз останніх досліджень та публікацій. В останніх дослідженнях були висвітлені переваги використання додатку Viber, та можливості спілкування шляхом даного месенджеру. Дослідивши використання вайберу було доведено, що це програмне забезпечення є важливим аспектом в розслідуванні кіберзлочинів. З'ясовано, що дослідження Viber в експертизі є важливою складовою для вилучення необхідних даних, для запобігання злочинів.

Формування цілей статті. Дослідити особливості мобільних месенджерів, виявити методи вилучення даних, з метою запобігання злочинів, та розглянути необхідність дослідження додатку Viber.

Виклад основного матеріалу. Щоб розглянути наше питання, з’ясуємо, що є месенджери, яка їх особливість. Під поняттям месенджер розуміється телекомунікація для обміну текстовими або відео повідомленнями між користувачами засобами мобільних пристроїв через Інтернет. Месенджери дозволяють швидко відправляти повідомлення, прослуховувати надіслані аудіо повідомлення, переглядати надіслані фотографії та орієнтуватися в тому, чи знаходиться ваш співрозмовник у мережі. Месенджер можна визначити як сповісник, повідомник. Користувачі додатків, при використанні різних месенджерів сповіщають, повідомляють певну інформацію іншому співрозмовнику, швидкими засобами спілкування. На даний час месенджери є безкоштовними мобільними додатками, для використання необхідно мати доступ до мережі Інтернет, що дозволяє швидко, зручно та безпечно спілкуватися. Також сучасні застосунки смартфонів дозволяють здійснювати відео дзвінки та дзвінки без витрат коштів, та охоплюють різні країни, з користувачами месенджерів яких можна спілкуватися. Використовуючи додатки є можливість організовувати розмови у групових чатах, або приватні розмови. Основною функцією месенджерів можна назвати обмін повідомленнями між користувачами, також це обмін медіафайлами та документами. Месенджери є важливими інструментами у сучасному світі цифрових технологій. Використання Viber, Facebook Messenger, Skype, Телеграм, Signal набувають широкого використання як серед молоді, так і серед людей літнього віку, які використовують смартфони та користуються мережею Інтернет. Згідно дослідженням Дж. Міда співрозмовники завдяки символів передають один одному інформацію, але символи- це не тільки знаки, але й взаємодія між людьми під час спілкування. Месенджерами

вважають мережу, яка побудована на певних програмах в Інтернеті. Ці мережі є взаємодією індивідуумів, за допомогою яких відбувається комунікація. Месенджери можна назвати соціальними мережами, які допомагають встановлювати зв'язки між різними групами людей та певними особами. Згідно теорії соціальних мереж, чим більше та міцніше користувачі спілкуються в месенджерах, тим активніше вони спілкуються у повсякденному житті. Комунікація по Інтернету розширює соціальну поведінку, тому чим тісніші контакти, тим частіше користувачі використовують будь то електронну пошту або різні додатки.

На початку 2000 років Інтернет месенджери набули великої популярності та з'явилися такі месенджери, які є популярними й досі, а саме LinkedIn, MySpace і Facebook. В цей час сталим є поняття «соціальна Інтернет мережа». З появою соціальних мереж комунікація набуває оперативності та глобальності.

Месенджери стали популярною платформою для спілкування. Кількість користувачів ними росте з кожним роком. Лідером серед додатків, які найбільше використовуються є Viber, яким користується 94% власників смартфонів. Facebook Messenger посідає почесне друге місце, а найменш поширеним додатком стає WhatsApp. Юзери Viber використовують застосунок майже 30 хвилин на день. При цьому користувачі використовують відеодзвінки, користуються стікерами, відправляють безліч повідомлень кожного дня. Науковці зацікавлені фактом використання месенджерів, які замінюють реальне спілкування. Додатки стали інструментом комунікації, де використовуються символи, розділові знаки, які підсилюють почуття та емоції. Візуальні символи створюють позитивне ставлення до повідомлення, тож смайлики теж широко використовуються в повідомленнях. При певних обставинах люди краще розуміють емоції один одного. Люди надсилають смайлики та наліпки, іноді це ефективніше, ніж сам текст.

Також застосунок Viber є важливим інструментом у розслідуванні різного роду злочинів, запобіганню корупції та вилучені дані з цього додатку можуть стати доказами в судових справах [5]. Вилучення даних залучають у кримінальних розслідуваннях, представляють як цифрові докази, при випадках шахрайства, кібератак.

Призначення та проведення судової експертизи є необхідною умовою для вирішення кримінального провадження. Судова комп’ютерно-технічна експертиза- це регламентована процесуальна дія, що проводиться в ході кримінальних правопорушень[2]. Вона є формою використання знань у галузі комп’ютерних технологій, а результати можуть бути частиною доказової бази.

Втрачені дані додатку можуть нести необхідну та важливу інформацію для розслідувань та для залучення у судових справах. Відновити дані можливо створивши резервну копію чатів. Це сприяє збереженню інформації на Google Drive для Android, та на iCloud для iPhone. Ця функція дає змогу швидко відновити всі чати та дату створення резервної копії. Всі особисті чати Viber зашифровані наскрізним шифруванням. Дані користувачів зберігаються на Amazon Web Services із дотриманням заходів безпеки, за умови резервного копіювання переписки зберігається у хмарному сховищі. Для збереження чатів необхідне постійне оновлення, в месенджері це відбувається автоматично. За допомогою резервної копії можна зберегти та відновити:

- історію чатів з текстовими повідомленнями та фото і відео файлами;
- участь користувача у групах та спільнотах;
- дані облікового запису;
- придбані стікери;
- тарифи та підписки Viber Out.

Для створення резервної копії на Android необхідно натиснути на три крапки в правому нижньому кутку «Додатково» - Параметри – Обліковий запис – Резервна копія Viber – обрати акаунт- «Створити резервну копію»[6]. Збереження резервної копії можна автоматично налаштувати з різною періодичністю. Це відноситься як для фото, так і для відео, завдяки мобільному Інтернету чи Wi-Fi. За допомогою резервної копії можливо відновити переписку користувача. Для цього відкриваємо Viber – натискаємо на три крапки в правому нижньому кутку «Додатково» - Параметри- Обліковий запис- Резервна копія Viber- «Відновити»- Підтвердити вибір «Відновити зараз». Про відновлення втрачених повідомлень слід подбати заздалегідь, розуміючи, що відновлення неможливе без резервного копіювання. Його можна проводити вручну або автоматично через обраний проміжок часу.

Якщо резервна копія відсутня, то можна скористатись програмами DiskDigger, EaseUS, Dr.Fone за допомогою яких, можна відновити втрачені фото та відеофайли. Для цього необхідно знати місце, де автоматично зберігаються медіафайли Viber при стандартних налаштуваннях на пристрої:

На пристроях під керуванням операційної системи Android застосунок Viber зберігає медіафайли у відкритому доступі в каталогах «Viber Video» та «Viber Images» за адресою /storage/emulated/0/Viber/ або /Internal Storage/Viber/

При дослідженні мобільних месенджерів та вилученні даних при вирішенні кримінальних розслідувань застосовується криміналістичне дослідження програми обміну повідомленнями[9]. Вся інформація зберігається в базі даних формату «SQLite». Інформація та додаткові файли бази даних і конфігураційні файли зберігаються в теці «viber.db».

- На пристроях під керуванням операційної системи Android застосунок Viber зберігає базу даних у внутрішній пам'яті пристрою, у спеціальному системному каталозі за адресою /data/data/com.viber.voip/database/ (для доступу потрібно мати root-права на пристрій);
- На пристроях під керуванням операційної системи iOS застосунок Viber зберігає свої дані в окремому контейнері /var/mobile/containers/data/application/[інікальний_ідентифікатор]/documents/ (для доступу потрібен jailbreak)

За допомогою спеціального програмного забезпечення «Oxygen Forensic Detective» або «Cellebrite Insecrets Physical Analyzer» можна отримати доступ до інформації:

- контакти користувача, імена та ідентифікатори Viber
- чати та текстові повідомлення, фото та відеофайли
- інформація про вхідні та вихідні дзвінки, здійснені через Viber
- налаштування приватності, звукові налаштування

Отримана інформація завдяки програмному забезпеченню допомагає виявити та зупинити кібератаки, ідентифікувати особу, з якою велася комунікація.

Висновки та перспективи подальших досліджень. У статті були виділені основні методи вилучення отриманих необхідних даних з додатків мобільних пристроїв та визначені найбільш ефективні методи для використання спеціалістами у професійній діяльності. В результаті нашого дослідження були виявлені комунікації в месенджерах, безпечно використання додатків мобільних пристроїв для користувачів різних вікових категорій.

У подальшому ми плануємо досліджувати месенджери, для виявлення даних у професійній сфері спеціалістами, продовжувати пошук методів дослідження та відслідкування нових месенджерів, що з'являються.

Література

1. Wynn J. Digital sociology: emergent technologies in the field and the classroom. Sociological Forum. 2009. 24 (2). URL: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1573-7861.2009.01109.x> (дата звернення: 08.05.2025).

2. Довженко О. Деякі питання призначення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. Науковий вісник Ужгородського національного університету. Серія «Право». 2019. Вип. 55. Т. 2. С. 124–127.

3. Словник термінів з кібербезпеки / за заг. ред. О.В. Копана, Є.Д. Скулиша. Київ : Аванпост-Прим, 2012. 214 с.

4. Степанюк Р. Л., Колесник В. Г. Судова комп'ютерно-технічна експертиза: стан і перспективи розвитку. Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2023. № 2 (102). С. 289–305. <https://doi.org/10.33766/2524-0323.102.289-305>.

5. Теплицький Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. Юридичний часопис Національної академії внутрішніх справ. 2019. № 18, 2. С. 24–32. <https://doi.org/10.33270/04191802.24>.

6. Комп'ютерно-технічні дослідження. URL: <https://ndekc.mk.ua/platni-posluhy/komp-iuterno-tekhnichni-doslidzhennia> (дата звернення: 08.05.2025).

7. Як зробити бекап і відновити переписку у Viber: інструкція. URL: <https://dev.ua/news/vinnytsia-1670327750> (дата звернення: 08.05.2025).

8. Як відновити історію чатів, контакти та файли Viber на телефоні з Android. URL: <https://recoverysoftware.com.ua/blog/how-to-recover-history-viber.html> (дата звернення: 08.05.2025).

9. Деактивація або видалення Viber на телефоні. URL: <https://help.viber.com/hc/uk/articles/9174583112861> (дата звернення: 08.05.2025).

References

1. Wynn J. Digital sociology: emergent technologies in the field and the classroom. *Sociological Forum*. 2009. 24 (2). URL: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1573-7861.2009.01109.x> (access date: 08.05.2025).

2. Dovzhenko O. Deiaki pytannia pryznachennia kompiuterno-tekhnichnoi ekspertyzy pid chas rozsliduvannia kiberzlochyniv. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii «Pravo»*. 2019. Vyp. 55. T. 2. S. 124–127.

3. Slovnnyk terminiv z kiberbezpeky / za zah. red. O.V. Kopana, Ye.D. Skulysha. Kyiv : Avanpost-Prym, 2012. 214 s.

4. Stepaniuk R. L., Kolesnyk V. H. Sudova kompiuterno-tekhnichna ekspertyza: stan i perspektyvy rozvytku. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E. O. Didorenka*. 2023. № 2 (102). S. 289–305. <https://doi.org/10.33766/2524-0323.102.289-305>.

5. Teplytskyi B. Zavdannia, obiekty ta pytannia kompiuterno-tekhnichnoi sudovoi ekspertyzy. *Yurydychnyi chasopys Natsionalnoi akademii vnutrishnikh sprav*. 2019. № 18, 2. S. 24–32. <https://doi.org/10.33270/04191802.24>.

6. Kompiuterno-tekhnichni doslidzhennia. URL: <https://ndekc.mk.ua/platni-posluhy/komp-iuterno-tekhnichni-doslidzhennia> (access date: 08.05.2025).

7. Yak zrobyty bekap i vidnovyty perepysku u Viber: instruktsiia. URL: <https://dev.ua/news/vinnytsia-1670327750> (access date: 08.05.2025).

8. Iak vidnovyty istoriiu chativ, kontakty ta faily Viber na telefoni z Android. URL: <https://recoverysoftware.com.ua/blog/how-to-recover-history-viber.html> (access date: 08.05.2025).

9. Deaktyvatsiia abo vydalennia Viber na telefoni. URL: <https://help.viber.com/hc/uk/articles/9174583112861> (access date: 08.05.2025).