генератора та його перевірка на предмет рівномірності розподілення ймовірності сформованих чисел.

***Список використаних джерел:***


1. Knuth D. E. The Art of Computer Programming, Volume 2: Seminumerical Algorithms, 3rd. ed., Boston, Mass, USA : Addison-Wesley, Longman Publishing, Addison-Wesley, Reading, Mass, 1998.
2. Mark A. Pinsky, Samuel Karlin. An Introduction to Stochastic Modeling, Fourth Edition., Academic Press, 2010.
3. Ahrens J. H., Dieter U., Grube A. Pseudo-random numbers. Computing 6 (1970) 121–138). URL: https://doi.org/10.1007/BF02241740.
4. Neumann J. von. Various techniques for use in connection w J. von Neumann. Various techniques for use in connection with random digits. Applied Math Series, Notes by G. E. Forsythe, in National Bureau of Standards, Vol. 12, 36–38, 1951.
5. Trevisan L. Extractors and Pseudorandom Generators 1999. Journal of the ACM URL: http://theory.stanford.edu/~trevisan/pubs/extractor-full.pdf



**Ключові слова:** комп'ютерне моделювання, метод Монте-Карло, метод зворотних функцій, генератори псевдовипадкових чисел, рандомізація.

**Key words:** computer modeling, Monte Carlo method, inverse function method, pseudo-random number generators, randomization.



***ЗАДЕРЕЙКО ОЛЕКСАНДР ВЛАДИСЛАВОВИЧ***

*Національний університет «Одеська юридична академія»,*
*доцент кафедри інформаційних технологій,*
*кандидат технічних наук, доцент*

***ЯНКОВСЬКИЙ ОЛЕГ ГЕОРГІЙОВИЧ***

*Національний університет «Одеська юридична академія»,*
*доцент кафедри інформаційних технологій,*
*кандидат технічних наук, доцент*

***ДИКА АНАСТАСІЯ ІВАНІВНА***

*Національний університет «Одеська юридична академія»,*
*асистент кафедри інформаційних технологій*


## ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ МЕСЕНДЖЕРА TELEGRAM

Велика кількість користувачів використовують для обміну інформацією різні месенджери. Однак далеко не всі користувачі віддають собі звіт у тому, наскільки є конфіденційним такий обмін інформацією

і хто саме може отримати доступ до метаданих користувача. Саме критерій конфіденційності повинен бути пріоритетним для кожного користувача, тому що він відображає, наскільки його метадані доступні «третій» стороні. При оцінці конфіденційності месенджерів необхідно враховувати наступні ключові вимоги:

1. Наявність постійного наскрізного шифрування, при якому ключі для розшифровки особистих повідомлень є тільки у відправника і одержувача.

2. Наявність відкритого вихідного коду месенджера, що дозволяє здійснити експертам аудит безпеки та виявити слабкі місця або уразливості в коді.

3. Наявність «зникаючих» повідомлень, які остаточно видаляються після закінчення встановленого користувачем періоду часу.

4. Наявність можливості збору метаданих про користувача власниками месенджера і сторонніми IT корпораціями;

5. Наявність комунікації месенджера з сервісами, які не мають прямого відношення до його базових серверів.

*Потенційні уразливості месенджера Telegram*

На концептуальному рівні месенджера Telegram існують нестандартні рішення, які змушують звернути увагу на заявлений його розробниками рівень конфіденційності і безпеки:

1) функція наскрізного шифрування повідомлень не використовується за замовчуванням, що є несподіваним сюрпризом для користувачів [1];

2) використання криптографічного протоколу MTProto власної розробки;

3) проблема «витік доступності» [2];

4) зберігання списків контактів з телефону/комп'ютера і інформації на серверах Telegram.

Заявлені розробником месенджера Telegram рішення обумовлюють початкову довіру користувачів до безпеки і захищеності його серверів. Однак, автору не вдалося знайти у відкритих джерелах інформації будь-яких даних про моніторинг мережевих з'єднань месенджера Telegram і їх подальшого аналізу, особливо з точки зору забезпечення конфіденційності користувачів.

Тому метою даного дослідження є аналіз вихідних з'єднань месенджера Telegram і підвищення рівня конфіденційності його користувачів.

Зазначимо, що найкращим варіантом організації комунікації будь-якого клієнтського програмного забезпечення, в тому числі і месенджерів, є безпосередня взаємодія його клієнтської частини з серверною (рис. 1) [3].

Виходячи з вище викладеного, автором був виконаний моніторинг всіх вихідних мережевих з'єднань, ініційованих клієнтською частиною месенджера Telegram протягом 120 діб і виконано їх подальший аудит.

Результати моніторингу вихідних мережевих з'єднань, ініційованих месенджером Telegram представлені в таблиці 1.

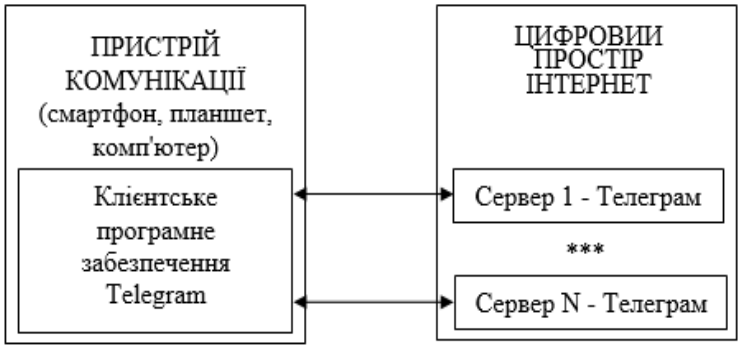


**Рис. 1. Безпечна комунікація клієнтського програмного забезпечення (месенджера Telegram)**

Таблиця 1 – Вихідні з'єднання месенджера Telegram

| **Власник** | **Доменне ім'я** | **IP-адреса,** | **Порт** | **Прото-кол** | **Стан** |
|---|---|---|---|---|---|
| Cloudflare | – | 104.16.249.249<br>104.16.248.249<br>2606:4700::6810:f8f9 | HTTP<br>HTTPS | TCP | Забл. |
| Leaseweb Asia Pacific pte | leaseweb.com | 85.113.71.220 | HTTPS | TCP | Забл. |
| Telegram Messenger Inc | telegram.org | 149.154.167.41<br>149.154.167.51<br>149.154.175.100<br>149.154.167.91<br>149.154.167.99<br>149.154.165.111<br>149.154.175.51<br>149.154.175.55 | HTTPS | TCP | Дозв. |
| | – | 91.108.56.192 | HTTPS | TCP | Дозв. |
| | – | 2001:67c:4e8:1033:3:100::a | HTTPS | TCP | Дозв. |
| | – | 2001:67c:4e8:1033:5:100::a | HTTPS | TCP | Дозв. |
| Google | ams15s21-in-f14.1e100.net | 216.58.212.142 | HTTPS | TCP | Забл. |
| | ams15s21-in-f4.1e100.net | 216.58.212.132 | HTTPS | TCP | Забл. |
| | waw.07s05-in-f3.1e100.net | 142.250.186.195 | HTTPS | TCP | Забл. |
| | waw.07s06-in-f14.1e100.net | 142.250.186.195 | HTTPS | TCP | Забл. |
| | waw.02s22-in-f4.1e100.net | 142.250.203.196 | HTTPS | TCP | Забл. |
| | waw.07s03-in-f10.1e100.net | 142.250.75.10 | HTTPS | TCP | Забл. |
| | zrh04s05-in-f106.1e.100.net | 172.217.18.106 | HTTPS | TCP | Забл. |

| Власник | Доменне ім’я | IP-адреса, | Порт | Прото-кол | Стан |
|---|---|---|---|---|---|
| | fra16s48-in-f10.1e.100.net | 142.250.185.74 | HTTPS | TCP | Забл. |
| | fra16s53-in-f4.1e.100.net | 142.250.185.228 | HTTPS | TCP | Забл. |
| | fra16s56-in-f4.1e.100.net | 142.250.181.228 | HTTPS | TCP | Забл. |
| | fra24s12-in-f10.1e.100.net | 142.250.184.234 | HTTPS | TCP | Забл. |
| | fra24s04-in-f14.1e100.net | 142.250.186.46 | HTTPS | TCP | Забл. |
| | fra16s52-in-f3.1e100.net | 142.250.185.195 | HTTPS | TCP | Забл. |
| | fra16s48-in-f3.1e100.net | 142.250.185.67 | HTTPS | TCP | Забл. |
| | fra16s49-in-f10.1e100.net | 142.250.185.106 | HTTPS | TCP | Забл. |
| | fra16s52-in-f10.1e100.net | 142.250.185.202 | HTTPS | TCP | Забл. |
| | fra16s53-in-f3.1e100.net | 142.250.185.227 | HTTPS | TCP | Забл. |
| | fra24s12-in-f4.1e100.net | 142.250.184.228 | HTTPS | TCP | Забл. |
| | fra16s50-in-f3.1e100.net | 142.250.185.131 | HTTPS | TCP | Забл. |
| | fra16s52-in-f14.1e100.net | 142.250.185.206 | HTTPS | TCP | Забл. |
| | fra16s56-in-f3.1e100.net | 142.250.181.227 | HTTPS | TCP | Забл. |
| | fra16s52-in-f4.1e100.net | 142.250.185.196 | HTTPS | TCP | Забл. |
| | fra24s06-in-f3.1e100.net | 142.250.186.99 | HTTPS | TCP | Забл. |
| | fra24s08-in-f10.1e100.net | 142.250.186.170 | HTTPS | TCP | Забл. |
| | fra16s51-in-f14.1e100.net | 142.250.185.174 | HTTPS | TCP | Забл. |
| | prg03s13-in-f3.1e100.net | 142.251.37.99 | HTTPS | TCP | Забл. |
| | prg03s12-in-f10.1e100.net | 142.251.36.138 | HTTPS | TCP | Забл. |
| | 82.221.107.34.bc.googleusercontent.com | 34.107.221.82 | HTTP | TCP | Забл. |
| | dns.google.com | 8.8.8.8 | DNS | UDP | Забл. |
| | | 8.8.4.4 | HTTPS | UDP | Забл. |
| | - | 2a00:1450:4001:82f::2003 | HTTPS | TCP | Забл. |
| | - | 2a00:1450:4001:811::200a | HTTPS | TCP | Забл. |
| | - | 2a00:1450:4001:800::200a | HTTPS | TCP | Забл. |
| | - | 2001:4860:4860::8888 | HTTPS | TCP | Забл. |
| | - | 2001:4860:4860::8844 | HTTPS | TCP | Забл. |

| Власник | Доменне ім'я | IP-адреса, | Порт | Про-токол | Стан |
|---|---|---|---|---|---|
| Akamai technologies | A104-89-25-202.deploy.static.akamaitechnologies.com | 104.89.25.202 | HTTPS | TCP | Забл. |
| | a104-92-88-65.deploy.static.akamaitechnologies.com | 104.92.88.65 | HTTPS | TCP | Забл. |
| | a104-111-214-42.deploy.static.akamaitechnologies.com | 104.111.214.42 | HTTPS | TCP | Забл. |
| | a104-90-179-34.deploy.static.akamaitechnologies.com | 104.90.179.34 | HTTPS | TCP | Забл. |
| | a2-18-12-41.deploy.static.akamaitechnologies.com | 2.18.12.41 | HTTPS | TCP | Забл. |

Візуальна інтерпретація вихідних з'єднань, отриманих у таблиці 1 наведена на рис. 2.

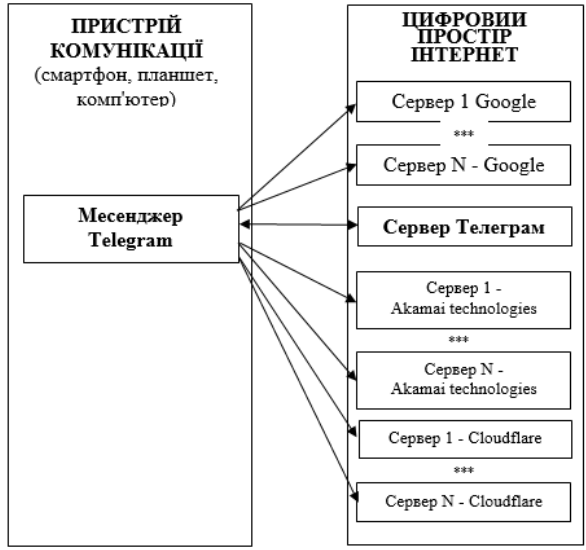


**Рис. 2. Візуальне представлення вихідних з'єднань месенджера Telegram зі сторонніми серверами IT корпорацій**

Аудит вихідних з'єднань з доменами та IP-адресами (див. табл. 1), ініційованих месенджером Telegram дозволив одержати такі дані:

– домен **.1e100.net* – підключений до ns-серверів *google.com*. Належить компанії Google;

– домен **.akamaitechnologies.com* – підключений до ns-серверів *akamaistream.net*. Належить компанії Akamai Technologies – провайдера платформи CDN і додатків для акселерації інтернет-додатків;

– домен *dns.google.com* – альтернативний DNS-сервер, розроблений корпорацією Google для прискорення завантаження веб-сторінок за рахунок підвищення ефективності кешування даних;

– домен **.bc.googleusercontent.com* – підключений до віртуальних машин корпорації Google в рамках проекту GCE;

– IP адреси 104.16.249.249, 104.16.248.249 – належать сервісу CDN Cloudflare корпорації Cloudflare Inc [4].

– Домен *leaseweb.com* – належить компанії Leaseweb, що надає послуги хмарного хостінгу, обробки даних, включаючи власну CDN.

*Аналіз отриманих даних*

Отримані результати моніторингу вихідного трафіку месенджера Telegram з цифровим простором Інтернет дозволили встановити факт ймовірного збору метаданих користувачів ІТ-корпораціями, які є лідерами на цифровому ринку обробки і монетизації даних користувачів. А саме:

2. Вихідні з'єднання з доменом **.bc.googleusercontent.com* обслуговуються віртуальними машинами класу GCE з використанням інфраструктури сервісу (IaaS) хмарної платформи Google, на яких можуть бути реалізовані телеграм-боти, в тому числі ті, що несуть шкідливий функціонал, з точки зору збору метаданих користувача [5; 6].

3. Вихідні з'єднання з сервісами доставки контенту CDN Cloudflare і Akamai Technologies являють собою гнучкий інструмент для отримання статистичних даних про користувачів: IP-адрес з яких запитується контент, пошукових запитів, кількість трафіку і т.д. [7].

4. Вихідні з'єднання з публічними DNS сервісами корпорації Google дозволяють їй контролювати весь DNS трафік ініційований месенджером Telegram [8; 9].

Результати виконаного аналізу вихідних з'єднань месенджера Telegram з цифровим простором Інтернет, обумовлюють необхідність блокування сторонніх з'єднань з сервісами ІТ корпорацій, для виключення ймовірного збору, аналізу, монетизації метаданих користувачів.

Для здійснення блокування вихідних з'єднань клієнтської частини месенджера Telegram необхідно використовувати міжмережеві екрани, які працюють на мережному пакетному рівні (рис. 3).

До їх числа можна віднести:

– для ОС Android – мережевий екран No Root Firewall [10];

– для сімейства ОС Windows – розширення вбудованого брандмауера Windows Firewall Control [11].

Висновки:

1. Блокування вихідних з'єднань месенджера Telegram зі сторонніми серверами ІТ корпорацій (див. табл. 1 і рис. 3) не призвело до втрати його функціоналу, закладеного розробником.

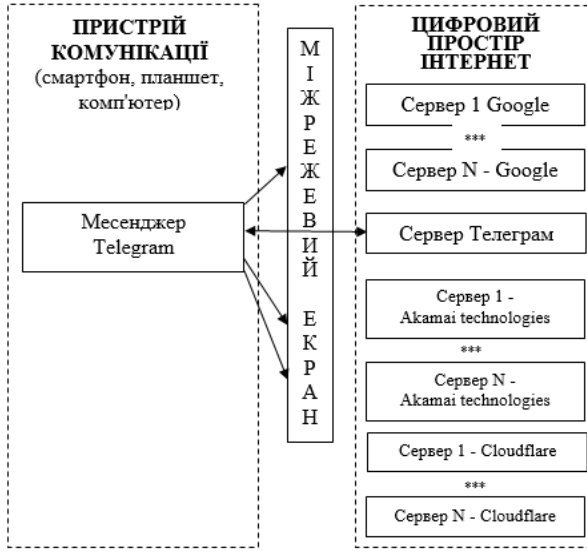


**Рис. 3. Вихідні з'єднання месенджера Telegram зі сторонніми серверами**

2. Блокування вихідних з'єднань месенджера Telegram зі сторонніми серверами ІТ корпорацій (див. рис. 3) викликало, незначне зниження швидкості завантаження проглядаємого медіаконтенту, що саме по собі неминуче через його завантаження безпосередньо з серверів месенджера Telegram.

3. Запропонований автором підхід дозволить уникнути імовірних витоків метаданих користувачів та підвищить конфіденційність користувачів месенджера Telegram на якісно новому рівні.

### *Список використаних джерел:*


1. Гасанова А. М. Телеграм-бот для гуртожитку на мові високого рівня програмування. – Дипломна робота на здобуття ступеня бакалавра спеціальності «Комп'ютерні науки», «Інформаційні управляючі системи та технології». – Національний авіаційний університет. – Київ, 2021. – 54 с.
2. Security Analysis of Telegram. URL: https://courses.csail.mit.edu/6.857/2017/project/19.pdf. (Дата звернення 5.06.2022).
3. Ots K. (2021). Network Security. In: Azure Security Handbook. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-7292-3_4.
4. Wingerath W. et al., "Speed Kit: A Polyglot & GDPR-Compliant Approach For Caching Personalized Content", 2020 IEEE 36th International Conference on Data Engineering (ICDE), 2020, pp. 1603–1608, doi: 10.1109/ICDE48307.2020.00142.
5. Salvi S., V Geetha. и Sowmya S. Kamath, "Jamura: A Conversational Smart Home Assistant Built on Telegram and Google Dialogflow", TENCON 2019–2019

IEEE Region 10 Conference (TENCON), 2019, стр. 1564–1571, doi: 10.1109 / TENCON.2019.8929316.
6. Bots in libr Bots in libraries: The aries: They're coming for coming for your jobs (or is it?) our jobs (or is it?). URL: https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=1142&context=library_research. (Дата звернення 5.06.2022).
7. Cdns' dark side: identifying security problems in cdn-to-origin connections. URL: https://users.encs.concordia.ca/~mmannan/student-resources/Thesis-MASc-Shobiri-2021.pdf. (accessed 5.06.2022). (Дата звернення 5.06.2022).
8. Abegaz B. W. DNS Services, alternative ways of using DNS infrastructures. – Delft: TNO, 2011. URL: https://repository.tudelft.nl/islandora/object/uuid:1e0114b7-d907-499e-bb20-fa83753d8067/datastream/URL/download. (Дата звернення 5.06.2022).
9. Задерейко О. В., Трофименко О. Г., Прокоп Ю. В., Логінова Н. І., Кухаренко С. В. Аналіз витоків даних у інформаційних системах. Сучасна спеціальна техніка. № 3 (66), 2021. С. 16-30.
10. NoRoot Firewall. URL: https://play.google.com/store/apps/details?hl=en&id=app.greyshirts.firewall. (Дата звернення 5.06.2022).
11. Windows Firewall Control. URL: https://binisoft.org/wfc. (Дата звернення 5.06.2022).

**Ключові слова:** месенджер Telegram, витоки метаданих в Telegram, вихідні мережеві з'єднання Telegram, конфіденційність месенджера Telegram.
**Key words:** Telegram messenger, Telegram metadata leaks, Telegram outgoing network connections, Telegram messenger privacy.

***ТОМА МАРІАНА ГЕОРГІЇВНА***

*Чернівецький національний університет імені Юрія Федьковича, асистент кафедри кримінального права, кандидат юридичних наук*

***БАЗАРНИЙ СЕРГІЙ ВАСИЛЬОВИЧ***

*Національний університет оборони України імені Івана Черняховського, підполковник, ад'юнкт кафедри застосування інформаційних технологій та інформаційної безпеки*

## ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В РЕАЛІЯХ МАСШТАБНОЇ ВІЙСЬКОВОЇ АГРЕСІЇ

Жахлива реальність сьогодення постає перед нашою країною з новими викликами та надскладними завданнями, які Україна зобов'язана виконати. Даючи гідну відсіч окупантам та різноплановим проявам гібридної війни, розпочатої Російською Федерацією ще у 2014 році, стає очевидним, що сьогодні Україна як суверенна держава зіштовхнулась з гострою нагальною необхідністю захисту фундаментальних націона-