КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.5978
УДК 004.057.2

Запорожець Валентина Юріївна
студентка кафедри захисту інформації
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0009-0006-6918-7784
valentyna.zaporozhets.kb.2022@lpnu.ua

Опірський Іван Романович
д.т.н., професор, завідувач кафедри захисту інформації
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

НЕБЕЗПЕКА ВИКОРИСТАННЯ TELEGRAM ТА ЙОГО ВПЛИВ НА УКРАЇНСЬКЕ СУСПІЛЬСТВО

Анотація. Стаття присвячена огляду багатоплатформового месенджера Telegram, дослідженню використання та огляду причин його надзвичайної популярності в Україні та наданню детальних методичних рекомендацій із забезпечення безпеки персональних даних користувачів у відповідності з останніми практиками у сфері кіберзахисту. В цій статті висвітлені основні проблеми популярного месенджера, починаючи з окремих пунктів політики конфіденційності цього застосунку, на прикладах показано, як йде збір конфіденційної інформації користувачів в сучасному цифровому середовищі через різноманітні чат-боти та інформаційні канали, показаний небезпечний вплив таких каналів на формування політичної думки українського суспільства; зроблений огляд власного алгоритму шифрування Telegram MTProto для звичайних чатів та секретних чатів з наскрізним шифруванням та визначено проблеми, пов'язані з шифруванням інформації на серверах компанії. Основну увагу стаття приділяє важливості захисту конфіденційних даних власників облікових записів месенджера Telegram. Зберігання та обробка даних такого виду потребує високого рівня безпеки, оскільки їхній несанкціонований витік чи порушення цілісності може призвести до викрадення іншого роду інформації, а також до втрати довіри користувачів. Досліджуються основні проблеми, з якими зіштовхуються користувачі застосунку Telegram у сфері кібербезпеки, та запропоновані ефективні підходи до їхнього вирішення шляхом безпечного мануального налаштування Telegram, а також надані рекомендації щодо коректного поводження з особистими даними користувачів з метою збереження їх конфіденційності та цілісності. Такий підхід дозволяє адаптуватися до постійно змінного оточення кіберзагроз і підвищує рівень захисту персональних даних фізичних осіб. Таким чином, аналізуючи перелічені вище аспекти, стаття надає читачам усвідомлення про небезпеку користування застосунком Telegram під час повномасштабної війни в Україні, допомагає усвідомити сучасні виклики в галузі кіберзахисту та надає детальні рекомендації для протидії цим викликам.

Ключові слова: Telegram; дані користувачів; чат-боти; інформаційні канали; викрадення інформації; MTProto; безпечне налаштування.

ВСТУП

Telegram, відомий як багатоплатформовий месенджер, було запущено до використання ще у 2013 році. В Україні широкого розповсюдження він набув з початком повномасштабного вторгнення росії. Зручний у використанні, зі зрозумілим інтерфейсом, легкодоступний месенджер швидко завоював довіру українських громадян.

Основними користувацькими функціями, які надає Telegram, є опціональні наскрізні зашифровані чати, відеодзвінки та обмін файлами [1]. Наразі месенджер використовують як для підтримання зв'язку всередині країни та за її кордонами, повідомлення про повітряні тривоги в моніторингових чатах, так і для проведення інформаційно-психологічних операцій, поширення дезінформації — перекручених, неповних або свідомо неправдивих відомостей для досягнення пропагандистської, військової, комерційної або іншої мети.

Відсутність критичного мислення в частини населення України і нехтування контролем над отриманням достовірної інформації сприяє появі великої кількості фейків, які поширюються в суспільстві.

Крім того, месенджер використовують для збору персональних даних користувачів. Персональні дані — це сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [2]. До персональних даних належить інформація: прізвище, ім'я та по батькові; національність; етнічне походження; дата й місце народження; паспортні дані; місце проживання; освіта; сімейний/майновий стан; релігійні переконання; політичні погляди; біометричні дані тощо. Саме ці дані можуть бути використані третьою стороною із злочинною метою.

Зважаючи на такі загрози, є потреба у розробленні рекомендацій щодо налаштування Telegram та навчанні населення правильного поводження з конфіденційною інформацією.

Постановка проблеми. У цій частині статті описується проблема, розгляду якої присвячене дослідження, вирішення якої матиме велике практичне значення для всіх користувачів застосунку. Розвиток технологій та швидке створення нових месенджерів, подібних Telegram, може поставити під загрозу дані користувачів, якщо вони не вмітимуть правильно використовувати ці засоби комунікації. Відповідно, розуміння користувачами небезпеки витоку даних зменшить ці ризики, а вміння розрізняти правдиву інформацію і фейки допоможе не створювати паніки та не демотивувати українське суспільство.

Аналіз останніх досліджень і публікацій. В нещодавно опублікованому дослідженні 2024 року щодо ринків викрадених даних було висвітлено, що Telegram містить угруповання для нерегульованого обміну конфіденційною інформацією. За визначену плату ці дані можуть бути отримані сторонніми особами. Актуальними проблемами на сьогодні залишаються велика кількість таких ринків та відсутність попереджень про них, адже нові ринки даних створюються досить швидко [3].

Ворожа пропаганда на сьогодні є однією з наймасштабніших проблем українського суспільсва. Напередодні повномасштабної війни проросійська пропаганда в постах Telegram-каналів поширювалася на 8,925% більше, а візуальна пропаганда — на 5,352% [4]. Стрімке підвищення кількості проросійських постів може свідчити про певні події, що можуть відбутися незабаром і це дає можливість прогнозувати їх.

Telegram часто хвалять за інноваційні успіхи, проте він викликав занепокоєння в користувачів щодо безпеки ще на початку його запуску. Експерти з кібербезпеки зі скептицизмом ставляться до достовірності інформації щодо роботи протоколу шифрування месенджера MTProto — його обмежена перевірка викликала критику. Сумніви викликали також наявність звичайних чатів, тобто тих, що не захищені наскрізним шифруванням, оскільки в альтернативах застосунку, таких як WhatsApp та Signal, тільки таке шифрування для всіх чатів. Підсумовуючи, виникає дилема, чи довіряти свої конфіденційні дані Telegram чи все ж таки дотримуватися принципу «Нікому не довіряти» у сфері безпеки даних [5].

Мета статті. Мета роботи полягає у проведені аналізу основних проблем Telegram щодо кібербезпеки, детальному огляді їх у статті. Додатково, метою статті є визначення рекомендацій щодо налаштування застосунку та безпеки поводження з месенджером

Завдання. Для успішного досягнення мети статті необхідно виконати наступні завдання:

- Провести детальний огляд Telegram і з'ясувати причини його популярності в Україні шляхом збору та аналізу актуальних офіційних даних та статистики щодо використання месенджера в Україні.
- Дослідити проблеми політики конфіденційності месенджера детальним розбором по окремих пунктах.
- Провести аналіз інформаційних каналів, які найбільш часто використовують для ІПСО шляхом аналізу статистики, та телеграм-ботів для збору особистих даних користувачів шляхом тестування.
- Зробити огляд протоколу шифрування Telegram MTProto та визначити проблеми, які пов'язані із відсутністю шифрування.
- Надати рекомендації щодо налаштування Telegram та щодо обміну даними для користувачів застосунку.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Огляд Telegram

Telegram (укр. Телеграм) є багатоплатформовим месенджером, що надає опціональні наскрізні зашифровані чати («секретні чати») та відеодзвінки, обмін файлами та деякі інші функції. Був запущений для iOS 14 серпня 2013 року та Android 20 жовтня 2013 року. Сервери Telegram розподілені по всьому світу з п'ятьма дата-центрами у різних частинах світу, а операційний центр базується в Дубаї, ОАЕ [6].

Офіційні компоненти Telegram мають відкритий вихідний код [7] за винятком сервера, який має закритий вихідний код і є власністю компанії [8]. Засновником і головою сервісу є російський програміст та бізнесмен Павло Дуров. Хмарні чати і групи шифруються між клієнтом і сервером, так що провайдери та інші треті сторони в мережі не можуть отримати доступ до даних. Користувачі можуть надсилати текстові та голосові повідомлення, здійснювати відео- та голосові дзвінки, обмінюватися необмеженою кількістю зображень, документами (2 ГБ на файл), місцезнаходженням користувача, анімованими наліпками, контактами та аудіофайлами. Користувачі також можуть стежити за каналами [8].

У січні 2021 року кількість активних користувачів Telegram перевищила 500 мільйонів щомісяця. У червні 2022 року Telegram перевищив 700 мільйонів щомісячних активних користувачів. Того ж місяця було запроваджено Telegram Premium — необов'язкову платну підписку з низкою додаткових функцій. У серпні 2023 року Telegram перевищив 800 мільйонів щомісячних активних користувачів. Станом на лютий 2024 месенджер налічує 900 млн користувачів (рис. 1) [9], [10].

Telegram випередив WhatsApp та Facebook Messenger і став найпопулярнішим додатком для обміну миттєвими повідомленнями в Азербайджані, Білорусі, Вірменії, Ефіопії, Йорданії, Казахстані, Камбоджі, Киргизстані, Молдові, Україні [11].

ISSN 2663 - 4023

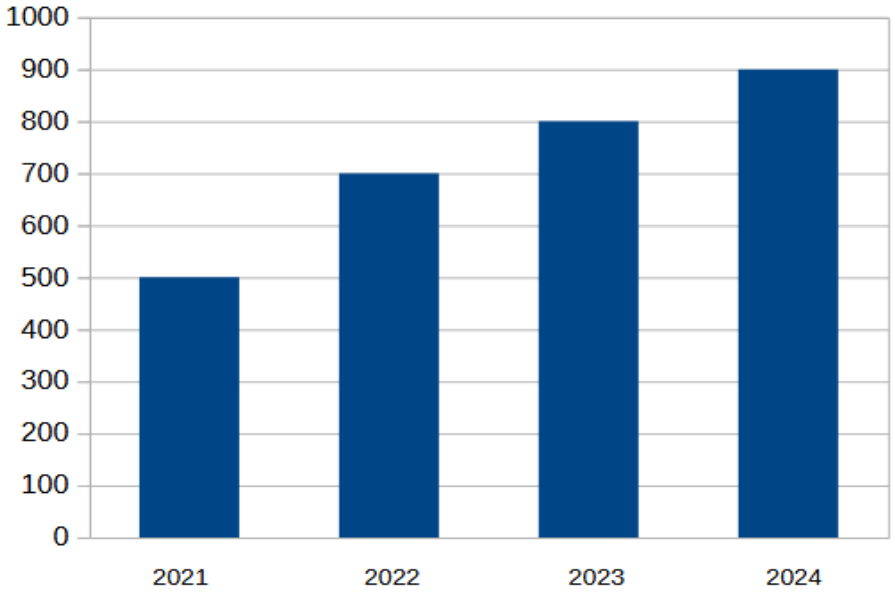

Рис. 1. Ріст кількості активних користувачів Telegram у млн. за 2021–2024 роки

Популярність в Україні

У квітні 2022 року Телеграм посів 6-ту сходинку за популярністю серед українських користувачів [12]. Із самого початку війни українці активно використовують цей застосунок. Ним також користується уряд для комунікації з населенням України, а також у цілях збору воєнних злочинів рф.

Як було зазначено в загальній інформації, додаток створив у 2013 році російський програміст Павло Дуров. Він був також співзасновником російської соцмережі «Вконтакте», яка наразі є заблокованою в Україні з 2017 року. Попри твердження про прозорість та безпечність застосунку, зв'язатися з офісом та потрапити туди фактично неможливо, оскільки месенджер не публікує вихідних даних. Відомо лише, що офіс Telegram працює в Об'єднаних Арабських Еміратах, що було зазначено в попередньому пункті.

Щодня українські користувачі приділяють застосунку щонайменше 40 хвилин, і до можливих причин росту популярності можна віднести:

1. Уряд держави створює інформаційні канали в Телеграмі, створюються боти для документування воєнних злочинів росії. Це і змушує людей залишатися в застосунку тривалий час. Прикладами таких чат-ботів є: WarCrime (для фіксації злочинів проти людяності з боку РФ під час війни в Україні), STOP Russian War (надання даних про перебування та пересування ворога й диверсантів) (рис. 2) Проте і ці чат-боти не захищені від необгрунтованого неочікуваного блокування як от в ніч з 28 на 29 квітня 2024 року, коли ГУР МО повідомило, що Telegram заблокував низку офіційних ботів, у тому числі й чат-боти української розвідки («єВорог», боти Головного управління розвідки та Служби безпеки). Через деякий час вони відновили роботу, проте досі залишається невідомим хто причетний до цього: керівництво компанії чи російська ФСБ. Саме ж керівництво Telegram повідомляє, що блокування сталося «помилково» [13]. Після таких нечітких коментарів від керівництва месенджера, довіра більшості користувачів помітно впала, а деякі взагалі обурені існуванням таких офіційних чат-ботів, адже, на їх думку, інформація одразу стає відомою ворогу.

Рис. 2. Телеграм-боти від уряду

2. Telegram дозволяє швидко надсилати повідомлення, передавати великі файли, має багато функцій для адміністрування каналів.

3. Українці використовують Телеграм задля спілкування із членами родини, що виїхали під час війни за кордон.

4. Зручний інтерфейс користувача, а також можливість зберігати контакти, вибрані повідомлення, налаштовувати персональний дизайн (рис. 3).

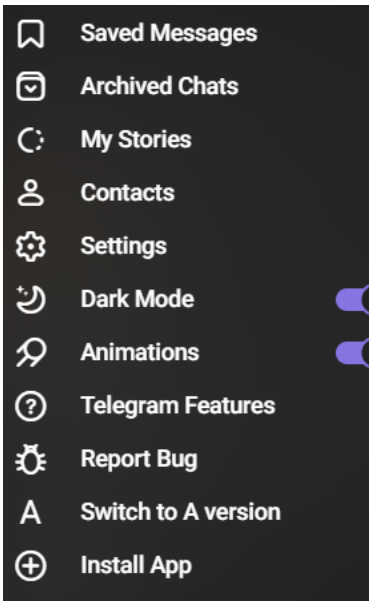

Рис. 3. Функціонал Telegram

Отже, популярність застосунку доволі висока. Але з ростом популярності і масштабності застосунку росте і кількість загроз, які наведемо в наступному пункті.

Проблеми політики конфіденційності Telegram

Аналіз проблем застосунку почнемо із тих правил, що були встановлені самою компанією, тобто з політики конфіденційності, якій більшість користувачів не надають важливого значення. В цьому пункті міститься цитований текст з політики конфіденційності Telegram [14], після нього відразу — підсумок і опис того, що викликає підозру.

Пункт 3.3.1 Хмарні чати

«Telegram — це хмарний сервіс. Ми зберігаємо на наших серверах повідомлення, фотографії, відео та документи з ваших *хмарних чатів*, щоб ви могли отримати доступ до своїх даних з будь-якого пристрою в будь-який час без необхідності покладатися на сторонні сервіси резервного копіювання. Усі дані зберігаються в надійно зашифрованому вигляді, а ключі шифрування зберігаються в кількох інших дата-центрах у різних юрисдикціях. Отже, місцевий технічний персонал або зловмисники (наприклад, у разі проникнення до дата-центру) не зможуть отримати доступ до даних користувачів».

Пункт 3.3.2 Секретні чати

«У *секретних чатах* використовується наскрізне шифрування. Це означає, що всі дані шифруються за допомогою ключа, яким володієте тільки ви й ваш співрозмовник. Ні ми, ні будь-хто інший без прямого доступу до вашого пристрою **не зможе** дізнатися, який вміст надсилається в цих повідомленнях. Ми не зберігаємо секретні чати на наших серверах. Ми також не ведемо жодних журналів повідомлень у секретних чатах, тому через короткий проміжок часу у нас не залишається інформації про те, з ким і коли ви спілкувалися в таких чатах. З тих же причин секретні чати недоступні в хмарі — ви можете отримати доступ до цих повідомлень лише з того пристрою, **з якого а**бо **на який** вони були надіслані».

Пункт 3.3.4 Публічні чати

«Окрім приватних повідомлень, Telegram також підтримує публічні канали та публічні групи. Усі публічні чати — це хмарні чати. Як і все в Telegram, дані, які ви розміщуєте в загальнодоступних спільнотах, шифруються як при зберіганні, так і при передачі — але все, що ви розміщуєте публічно, буде доступне всім користувачам».

Підсумовуючи пункти політики конфіденційності щодо чатів, можна виділити:

- хмарні чати зберігаються на серверах компанії в надійно зашифрованому вигляді;
- секретні чати на серверах не зберігають;
- публічні чати шифруються, але інформація публікується для всіх.

Пункт 3.5 Дані про місце розташування

«Якщо ви ділитеся своїм розташуванням у чаті, ці дані обробляються так само, як і інші повідомлення в хмарних або секретних чатах відповідно. Якщо ви транслюєте своє місце розташування (функція «Маячок») у будь-якому чаті або вмикаєте функцію «Показати мене» у розділі «Люди поблизу», Telegram використовуватиме ваші дані, щоб показувати ваше розташування тим користувачам, з якими ви ним ділитеся, навіть коли застосунок закритий — доки ви тримаєте ці додаткові функції активованими».

Підсумок: ваше місце розташування ви надаєте під власну відповідальність.

Пункт 4.1 Зберігання даних

«Якщо ви зареєструвалися в Telegram з Європи, ваші дані зберігаються в дата-центрах у Нідерландах. Ці дата-центри належать стороннім організаціям, у яких Telegram орендує призначений простір. Однак сервери та мережі, які знаходяться в цих дата-центрах і на яких зберігаються ваші персональні дані, належать Telegram. Ми не передаємо ваші персональні дані таким дата-центрам. Усі дані зберігаються в надійно зашифрованому вигляді, тому місцевий технічний персонал Telegram або зловмисники (наприклад, у разі проникнення до дата-центру) не можуть отримати до них доступ».

У підсумку маємо: дані зашифровані. Але у випадку відсутності шифрування є загроза викрадення даних зловмисником, що може бути працівником дата-центру або видаватиме себе за нього. Про сторонні організації та дата-центри теж інформації немає, що викликає сумнів щодо того, чи дійсно конфіденційні дані знаходяться в безпеці.

Пункт 5.2 Безпека та захист

«Telegram підтримує величезні спільноти, які ми маємо контролювати, щоб запобігти зловживанню й порушенню Умов використання. Крім того, Telegram має понад 700 мільйонів користувачів, що робить його привабливою ціллю для зловмисників. Задля підвищення безпеки вашого облікового запису, а також щоб запобігти спаму, зловживанню та іншим порушенням наших Умов використання, ми

можемо збирати метадані, такі як: ваша IP-адреса, відомості про пристрої та застосунки Telegram, які ви використовували, історія змін імені користувача тощо. У разі, якщо такі метадані були зібрані, вони можуть зберігатися не більше 12 місяців».

Підсумок: ми надаємо дозвіл на тимчасове зберігання наших метаданих для сумнівних цілей.

Пункт 6.2 Способи отримання даних ботами

«Розробники ботів можуть отримати ваші дані, коли ви взаємодієте з ботами, а саме:

- надсилаєте повідомлення боту;
- використовуєте вбудованого;
- є учасником групи, в яку додано бота;
- натискаєте на кнопки в повідомленнях, надісланих ботом;
- оплачуєте товари та послуги через бота».

Пункт 6.4 Сторонні боти не залежать від Telegram

«Окрім наших власних ботів, жодні інші боти або сторонні розробники ботів не пов’язані з Telegram. Вони повністю незалежні від нас. Вони повинні запитати у вас дозволу, перш ніж отримати доступ до ваших даних або даних від вас».

Маємо наступне: в застосунку існують боти, і при взаємодії з ними повну відповідальність за наші дані несемо ми.

Пункт 8.2 Компанії групи Telegram

«Для надання, вдосконалення та підтримки наших Послуг ми можемо передавати ваші персональні дані: нашій материнській компанії Telegram Group Inc., зареєстрованій на Британських Віргінських островах, Telegraph Inc., компанією групи Telegram, також зареєстрованою на БВО, і Telegram FZ-LLC, компанією групи Telegram, зареєстрованою в Дубаї. Ми вживаємо відповідних заходів для забезпечення безпеки та збереження цих персональних даних, що означає застосування стандартних договірних положень (*Standard Contractual Clauses*), затверджених Європейською комісією, в угодах з іншими компаніями групи Telegram».

Ми надаємо дозвіл на передавання наших даних материнській та дочірнім компаніям, але невідомо чи це дійсно безпечно.

Пункт 10.2 Повідомлення

«У хмарних чатах ви можете видалити повідомлення для всіх учасників протягом щонайменше 48 годин після відправлення. Якщо пройшло більше ніж 48 годин, видалення повідомлення видалить його лише з вашої історії повідомлень, а його копія залишиться на сервері як частина історії повідомлень вашого співрозмовника. Як тільки ваш співрозмовник також видалить його, воно зникне назавжди».

Висновок: копії видалених лише у вас повідомлень зберігаються на серверах компанії.

Проаналізувавши політику конфіденційності, ми визначили основні пункти, до яких виникають запитання, оскільки деякі твердження піддаються сумнівам. Причину таких сумнівів розглянемо в наступних пунктах.

Інформаційні канали для ІПСО та телеграм-боти для збору даних

Telegram активно використовують для поширення російської пропаганди. Її теми дещо змінюються з часом. Цю динаміку відстежує та показує Центр стратегічних комунікацій та інформаційної безпеки. Але основні напрямки поширення пропаганди такі (рис. 4):

ISSN 2663 - 4023

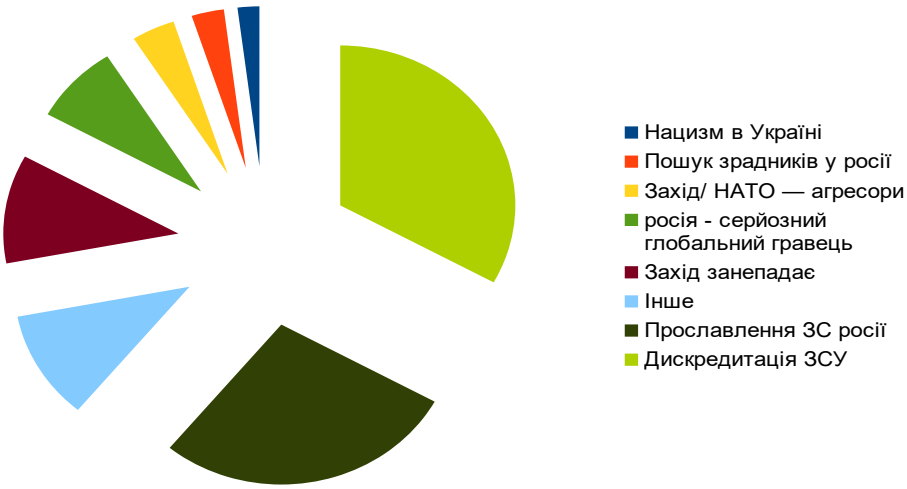

Рис. 4. Інфографіка тем кремлівської пропаганди у червні згідно з Центром стратегічних комунікацій та інформаційної безпеки

Все це робиться з метою дезінформувати українське суспільство, змусити за допомогою психологічного впливу повірити, що споживається «таємний український контент», а також загострити ситуацію в країні. Потрапити в цю пастку може будь-яка особа. Це може викликати паніку в суспільстві, спричинити хаотичні дії, або відволікти від інших, більш важливих новин.

Так як достовірність інформації на каналах часто оцінюється кількістю підписників, яку легко підняти штучно до високої чисельності, інформація починає ширитися Україною. Поширення проросійських публікацій можна прослідкувати за схемою від ЛІГА.net [9], в якій наведено перелік тих інформаційних псевдоукраїнських каналів, що поширюють фейки (рис. 5).

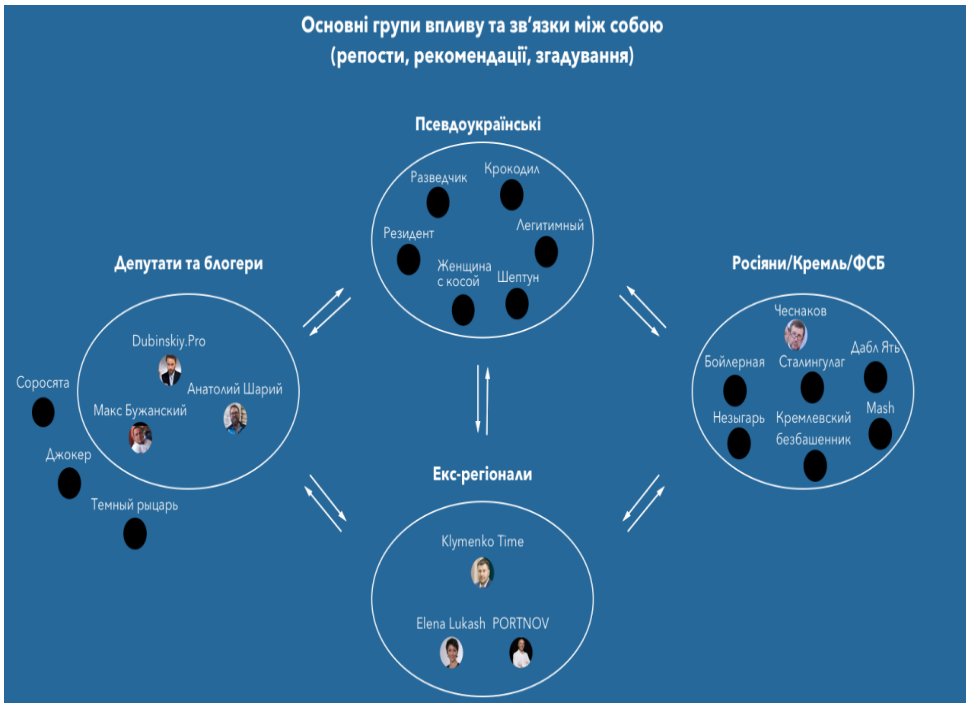

Рис. 5. Схема від ЛІГА.net щодо поширення проросійських публікацій

ISSN 2663 - 4023

Неприємні ситуації навколо збереження персональних даних пов'язані також з тим, що у Telegram є канали чи/та боти, в яких можна було придбати персональні дані українців. Ці канали та боти швидко закривають, проте проблема досі актуальна.

Ми вивчили декілька таких ботів, які містять на інформацію про українців. Власники цих ботів невідомі, у деяких — оплата лише в рублях або через російські пеймент-процесори [15].

@info_baza_bot (Info_baza) (рис.6).

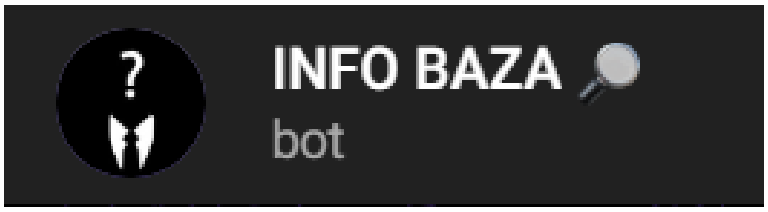

Рис. 6. INFO BAZA bot

Бот шукає людину в Україні за ПІБ, фото, номером телефону, правами водія або електронною адресою. База містить 420 000 користувачів, 70 млн номерів та 20 млн українських email-адрес.

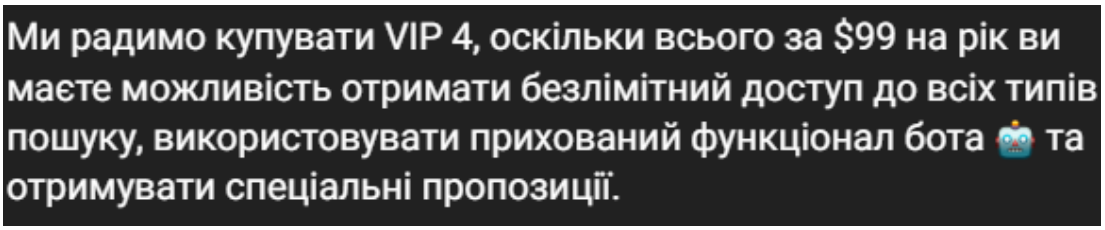

Рис. 7. Підписка на бот

VIP-пакети (вартістю $99 на рік) надають безлімітний пошук (рис. 7). Також VIP-доступ можна отримати, запросивши щонайменше 50 друзів. Приклад даних, що отримаємо з бота (рис. 8).

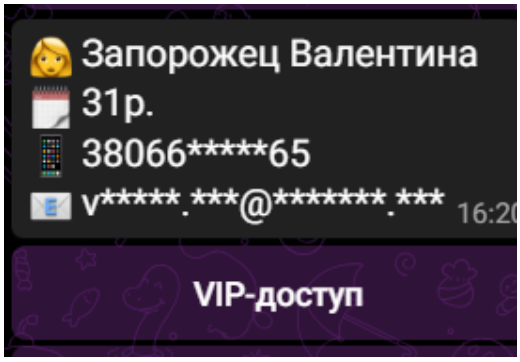

Рис. 8. Дані, отримані з бота INFO BAZA

ISSN 2663 - 4023

@Smart_SearchBot (SmartSearchBot) — альтернатива Info_baza. За поштою можна дізнатися телефон, ПІБ та дату народження. Вартість варіюється від $0,9 за добу до $30 за рік. Приклад отримання даних (рис. 9).

Рис. 9. Дані, отримані з бота SmartSearchBot

@telesint_bot (TeleSINT) — бот надає інформацію про участь користувачів Telegram у відкритих та закритих групах. Пошук — за вказаним в месенджері іменем. 3 запити безкоштовні (рис. 10–11).

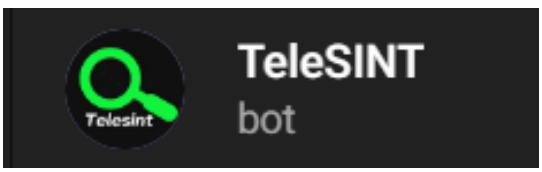

Рис. 10. Бот TeleSINT

ISSN 2663 - 4023

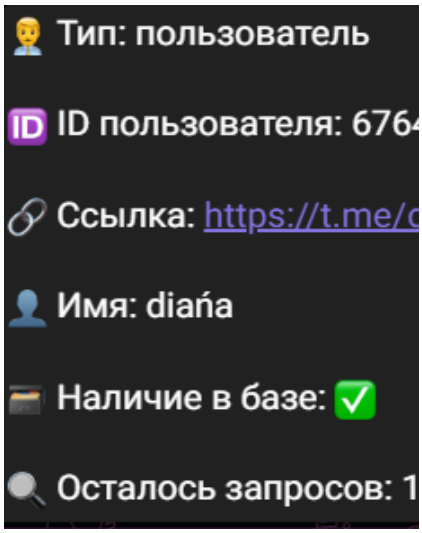

Рис. 11. Приклад отриманих даних з бота TeleSINT

Отже, знаючи ПІБ людини, ми можемо дізнатися її дату народження, телефони та пошти, номер паспорту, ІПН, дані про нерухомість та наявність ФОП, навіть паролі до пошти, а також геолокацію та групи Телеграм, де людина є учасником.

Шифрування

Перш ніж розглядати цю тему, зазначимо: згідно із законами росії, при зборі персональних даних росіян компанія зобов'язана зберігати їх на серверах на її території, тож Telegram також має сервери у цій країні. Тепер безпосередньо до теми.

Експерт з кібербезпеки, Костянтин Корсун говорить про шифрування Telegram так:

«Навіть якщо увімкнути ось ці секретні чати, то і тут є сумніви стосовно того, наскільки це безпечно, тому що сама компанія Telegram сама розробила свій власний криптографічний протокол MTProto і стосовно його безпечності є великі сумніви. Чому. Тому що той самий Signal, WhatsApp, Facebook Massanger і навіть Viber використовують розроблений криптографічний протокол, який відкритий і публічний. Кожен фахівець може зайти і подивитися чи все з ним гаразд, чого немає наприклад у Telegram. Цей протокол повністю закритий, Дуров його нікому не показує, але завіряє, що все безпечно...»

Рис. 12 показує клієнт-серверне шифрування. Коротко про те, як виглядає MTProto.

В загальному, воно полягає в тому, що збирається пакет для шифрування, що складається з server salt (випадкового 64-бітного числа, яке змінюється кожні 30 хвилин окремо для кожної сесії за запитом сервера), ідентифікатора сесії (випадкового 64-бітного числа, що генеруються клієнтом з метою розрізняти окремі сеанси одного користувача), корисного навантаження (до нього включені час, довжина та номер сегмента, які перевіряються на стороні одержувача) та заповнення (додавання даних до інформації задля забезпечення криптостійкості).

Далі знаходиться ключ повідомлення, 128 середніх біта хеша (SHA-256) від повідомлення з додаванням 32-байтового фрагмента ключа авторизації. Ключ авторизації у комбінації з новознайденим ключем повідомлення визначає за допомогою функції формування ключа 256-бітний ключ AES та 256-бітний ініціалізаційний вектор. Далі знайдені значення ключа AES та ініціалізаційного вектора використовуються в алгоритмі AES IGE для шифрування повідомлення. Наприкінці збирається пакет, що складається із зовнішнього загаловку, а також із зашифрованого повідомлення.

ISSN 2663 - 4023

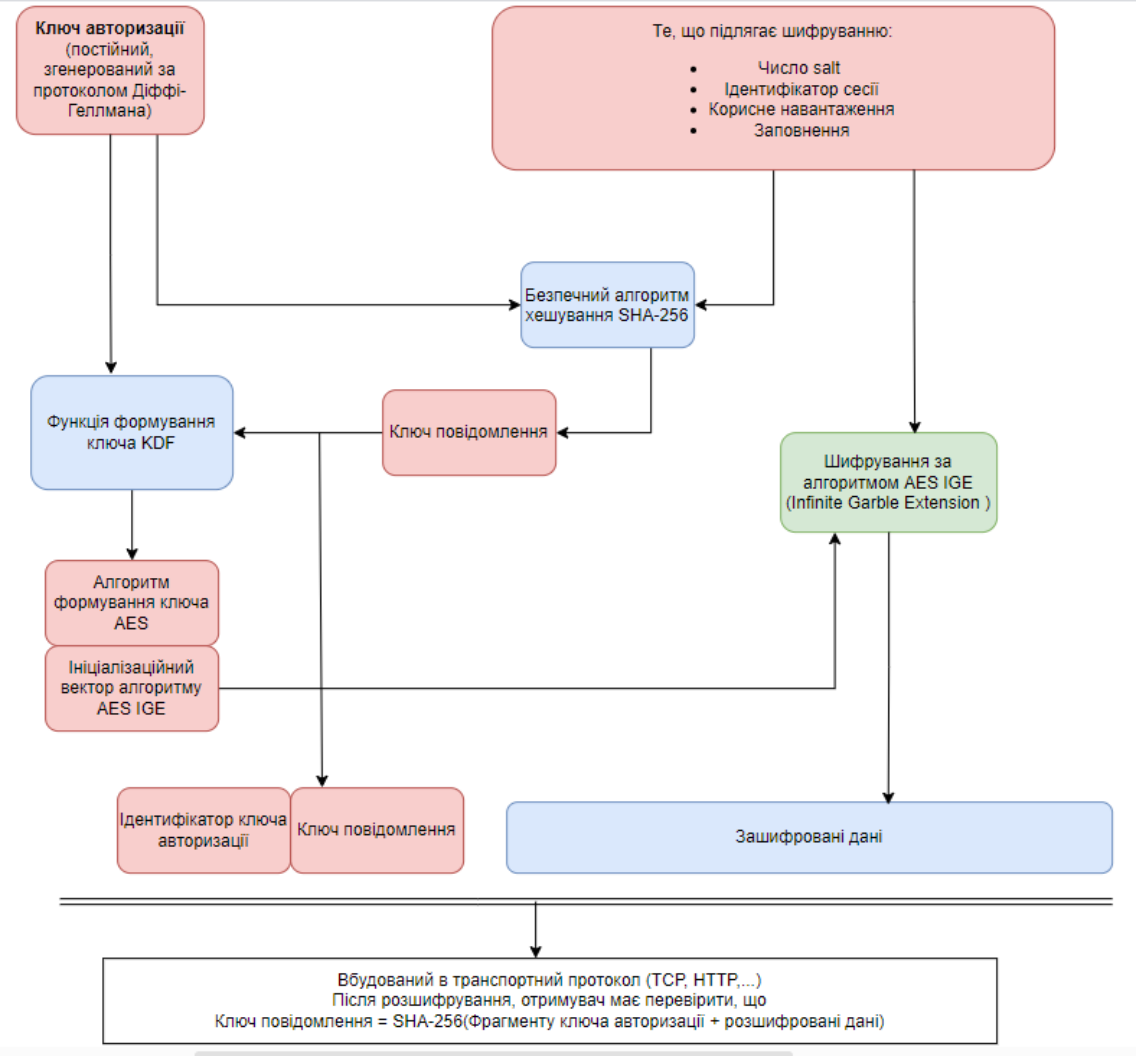

Рис. 12. Схема роботи MTProto в хмарних чатах

В секретних чатах шифрування (рис. 13) полягає в тому, що по черзі виконуються два ідентичні шифрування з різними ключами — секретним та авторизаційним. Нам потрібно отримати секретний ключ, але так, щоб ніхто і ніколи не його не дізнався. В цьому також допомагає алгоритм Діффі-Геллмана.

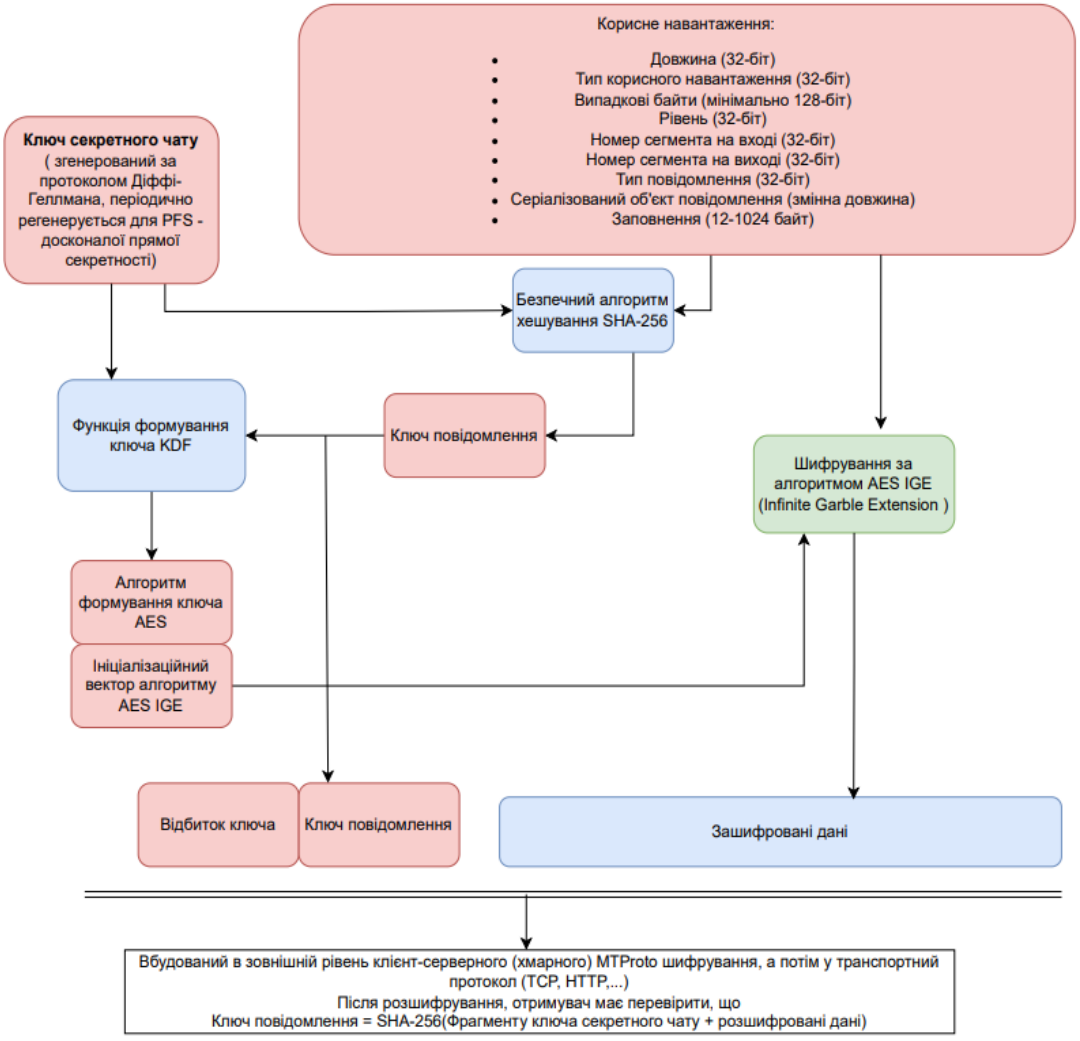

Рис. 13. Схема роботи MTProto в секретних чатах

Проте, незважаючи на існування цього алгоритму шифрування, виникає дуже багато проблем.

Засновник месенджера Signal заявив, що Telegram зберігає у незашифрованому вигляді на своїх серверах усі контакти користувачів, передані файли та всі отримані і надіслані повідомлення [16]. Це можна перевірити власноруч. Якщо взяти новий телефон, встановити на нього Telegram і увійти до свого аккаунту, ви побачите все своє попереднє листування.

Керівник служби підтримки Telegram Маркус Ра [17] підтвердив, що хмарні чати месенджера, збережені на серверах, можуть бути розшифровані працівниками компанії.

За даними самого Telegram, для захисту даних, незашифрованих наскрізним шифруванням, месенджер використовує розподілену інфраструктуру, тобто дані хмарних чатів зберігаються у різних дата-центрах (згідно п. 4.1. політики конфіденційності Telegram), а ключі шифрування розділені на частини та не зберігаються в одному місці із даними, які вони захищають. Отже той, хто має доступ до інфраструктури месенджера, все ж може розшифрувати збережені чати.

Зауваження є також і щодо секретних чатів. При надсиланні адреси сайту чи відеоматеріалу з посиланням, у чаті з'являється скріншот цього посилання. Це свідчить про те, що Telegram створює попередній перегляд посилань на власних серверах, як для

звичайних, так і для секретних чатів. Це вже суперечить сенсу секретного чату, адже політика конфіденційності інформує, що сервери не переглядають і не зберігають інформацію в чатах цього типу.

Також, не розглядаючи саме шифрування, збір даних може вестись також і простим способом — спостереження за часом входу в месенджер. Наприклад, маємо групу з 30 осіб, всі вони не мають прихованого статусу останнього відвідування. Наприклад, час останнього відвідування в першої, другої та третьої особи — 15:43 15:43 та 15:44 відповідно. На основі цих даних робимо висновок, що є висока ймовірність того, що ці особи нещодавно спілкувалися один з одним в певній приватній чи публічній групі.

Зробивши такий аналіз, доходимо до висновку, що найкращий варіант — змінити месенджер на альтернативний йому з нормальним шифруванням і відкритим кодом, такий як наприклад Signal. Порівняно з Telegram безпечнішими месенджерами також є Viber, WhatsApp чи Facebook Messenger.

Але якщо в користуванні Telegram є необхідність, то треба це робити правильно та з піклуванням про власну безпеку. В наступному пункті розглянемо рекомендації щодо його налаштування.

Детальні рекомендації щодо налаштування Telegram та рекомендації щодо обміну даними

В ході дослідження було визначено, що найголовнішою проблемою безпеки є те, що люди самі надають про себе інформацію, тож розглянемо деякі пункти, які допоможуть зберегти користувачам конфіденційність їхніх даних.

1. При реєстрації в Telegram небажано вказувати свій номер телефону, за яким у користувача є прив’язка до банківських карток, інших важливих облікових записів. Цей пункт необов’язковий, але бажаний: обирати для месенджера слід інший, спеціальний для цього, номер телефону.

2. При створенні облікового запису в Telegram небажано вказувати своє справжнє ім’я та прізвище. В описі не слід вказувати персональних даних. Нещодавнє оновлення застосунку пропонує користувачу ввести дату народження — не слід робити цього також. Своє фото теж бажано не ставити. Оскільки, як було описано в розділі про боти, збирається все — починаючи від імені і опису, закінчуючи фотографією профілю.

3. Якщо фото профілю встановлене і воно ідентифікує користувача, то його слід зробити невидимим для інших користувачів, номер телефон також приховати.

4. Не слід вмикати геолокацію для виявлення людей поблизу.

Розглянемо рекомендації щодо технічних налаштувань:

При створенні активного облікового запису, слід подбати про налаштування чатів. Необхідно зайти в меню і обрати «Налаштування». В налаштуваннях обрати «Налаштування чатів». Прокрутивши донизу, вимикаємо пункт «Вбудований браузер» (рис. 14), щоб сервер не «читав» наші повідомлення.

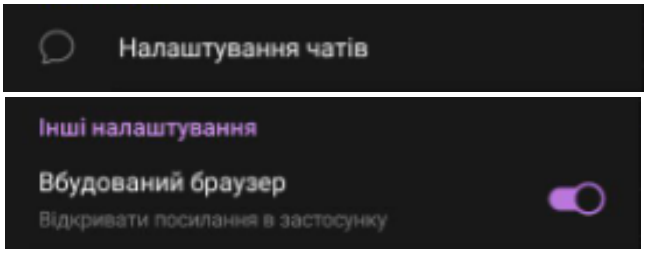

Рис. 14. Увімкнений вбудований браузер в «Налаштуваннях чатів»

Наступним кроком треба забезпечити відносно надійний захист. В меню слід обрати «Налаштування», а там — розділ «Приватність і безпека» (рис. 15).

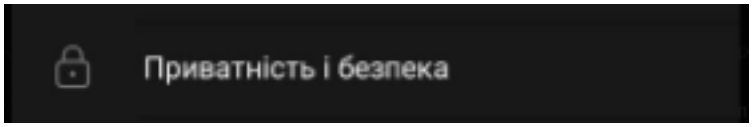

Рис. 15. Налаштування приватності і безпеки

Двоетапна перевірка обов'язково має бути увімкнена. По можливості можна вибрати «Видалення за таймером». Це дозволить застосунку автоматично видаляти повідомлення у обох користувачів, без можливості повернути їх.

Обов'язково має стояти код блокування. І обов'язково має бути прихований номер телефону, фото, остання активність, заборонене пересилання повідомлень. Бажано від усіх. Від контактів теж. Адже у випадку викрадення їх облікового запису, номер телефону, зовнішній вигляд, останній час відвідування користувача бачитиме зловмисник. А дозволене пересилання повідомлень не бажане, оскільки це призведе до того, що люди в публічних чатах зможуть бачити профіль за посиланням.

На наступному рисунку (рис. 16) показаний обліковий запис звичайного користувача, відповідальність якого щодо власної безпеки знаходиться на початковому рівні, оскільки двоетапну перевірку та код блокування не встановлено. Приватність відносно правильно налаштована.

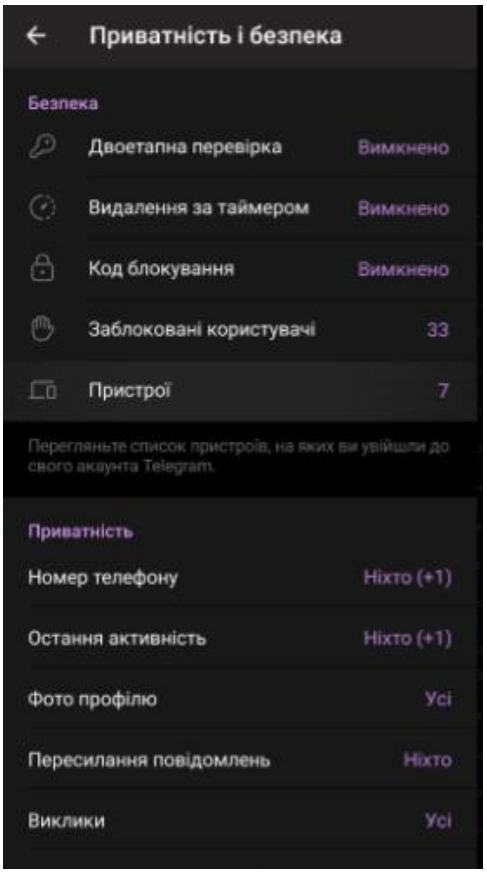

Рис. 16. Налаштування приватності і безпеки звичайного користувача

ISSN 2663 - 4023

Хоча тут синхронізація увімкнена, контакти синхронізувати також не бажано. Попередній перегляд посилань обов'язково вимикаємо.

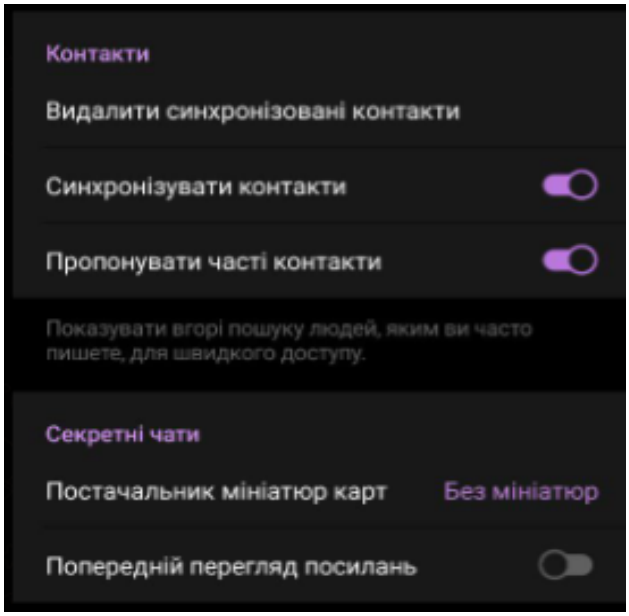

Рис. 17. Вимкнений перегляд посилань

На цьому відносно безпечне мануальне налаштування завершено.

Є також декілька рекомендацій стосовно підвищення рівня безпеки, які стосуються раціонального обміну даними. Ту запропонуємо наступні методи:

- Не слід пересилати в Telegram інформацію, яка стосується банківських карток, рахунків, особисту інформацію, таку як паспортні дані, ідентифікаційний код. Ніякі інші коди доступу чи паролі зберігати в месенджері теж не слід. Ніякою такою інформацією не слід ділитися навіть з близькими — у переписці можлива присутність зловмисника-наглядача, який потім може використати цю інформацію в зловмисних цілях.
- Зображення, відеоповідомлення, і загалом те, що містить інформацію про користувача, але яку він хоче надіслати, слід архівувати за допомогою архіваторів (7Zip, WinRar і т.п.)Так підвищиться рівень безпеки користувача, а також осіб, які знаходяться на зображеннях та відеоматеріалах.
- Ніколи не слід надсилати в повідомленнях адресу чи поточне місцезнаходження. (Загалом це попередження спочатку стосувалося військових, адже Telegram має деякі зв'язки із росією, і це може нашкодити державним та військовим інтересам України. Зараз це стосується також і цивільних, оскільки вони несвідомо можуть стати коригувальниками вогню для окупантів).
- Слід намагатися використовувати месенджер тільки для загальних речей. Не рекомендовано його використання для бізнес-розмов, планування великих зустрічей. Все це обумовлено тим, що терористичні організації також наявні в месенджері і вони теж можуть виступати зловмисниками, що прослуховують чи перечитують повідомлення. Якщо їхньою метою буде масове убивство, то воно може відбутися через те, що зловмисникам буде відоме місце та час зібрання.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Подана стаття детально досліджує проблеми безпеки Telegram, зосереджуючись на теоретичному рівні. Підсумовуючи дослідження, можна визначити деякі аспекти: Telegram хоч і є зручним в користуванні чи доступі для багатьох, він не є безпечним. Нам не відомо, що приховується за алгоритмом шифрування MTProto і чи знаходяться на даний момент конфіденційні дані в безпеці. Невідомо й те, чи зможуть сторонні особи збирати наші дані у будь-який момент, адже невідомо наскільки добре реалізований захист серверів.

Політика конфіденційності, що надає нам «гарантії безпеки», складена абстрактно, а практичний функціонал застосунку часто різниться із заявленим.

Деякі телеграм-канали та боти приховують у собі зловмисний вплив на українське суспільство та можливість витоку конфіденційних даних, а існування в месенджері секретних чатів не має сенсу, оскільки серверами здійснюється і їхній перегляд.

Надані в дослідженні рекомендації щодо налаштування застосунку та щодо обміну даними в ньому допоможуть при використанні Telegram запобігти витоку даних та збору будь-якого виду інформації. Проте, задля почуття в безпеці рекомендовано перестати використовувати Telegram і перейти на більш безпечні альтернативи, такі як WhatsApp чи Signal.

Результати дослідження в майбутньому може бути використано для вивчення проблем безпеки месенджера на практичному рівні, з поглибленим дослідженням технічних аспектів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *The Next Web.* (n. d.). *Telegram introduces end-to-end encrypted video calls.* https://thenextweb.com/news/telegram-introduces-end-to-end-encrypted-video-calls/
2. *Стаття 2 Закону України «Про захист персональних даних».* (n. d.). https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Garkava, T., Moneva, A., & Leukfeldt, E. R. (2024). Stolen data markets on Telegram: a crime script analysis and situational crime prevention measures. *Trends Organ Crim*. https://doi.org/10.1007/s12117-024-09532-6
4. Theisen, W., et al. (2024). An Avalanche of Images on Telegram Preceded Russia's Full-Scale Invasion of Ukraine. *arXiv.* https://doi.org/10.48550/arXiv.2402.14947
5. Komiljonov, J. (2024). How Safe Telegram Is to Keep Personal Data and Conversations. *EUROPEAN JOURNAL OF BUSINESS STARTUPS AND OPEN SOCIETY, 4(2),* 54–57.
6. *The Evolution of Telegram.* (n. d.). https://telegram.org/evolution#october-2013
7. Witman, E. (2021). *How to make a Telegram account and start using the popular group chatting app*. *Business Insider*. https://www.businessinsider.com/guides/tech/how-to-make-a-telegram-account
8. *List of Telegram applications.* (n. d.). https://telegram.org
9. *Durov's Channel.* (n. d.). https://t.me/durov/148
10. Буняк, В. (2024). *Дуров в інтерв'ю Financial Times: Кількість користувачів телеграму сягнула 900 мільйонів у лютому 2024 року.* https://ms.detector.media/trendi/post/34401/2024-03-11-durov-v-intervyu-financial-times-kilkist-korystuvachiv-telegramu-syagnula-900-milyoniv-u-lyutomu-2024-roku/
11. Most Popular Messaging Apps by Country — Similarweb. (n. d.). https://www.similarweb.com/blog/research/market-research/worldwide-messaging-apps
12. Кудіна, М. (n. d.). *Telegram: чому він такий популярний серед українців та які небезпеки приховує.* https://netfreedom.org.ua/article/telegram-chomu-vin-takij-populyarnij-sered-ukrayinciv-ta-yaki-nebezpeki-prihovuye
13. Москаленко, Ю. (n. d.). *TELEGRAM РОЗБЛОКУВАВ ОФІЦІЙНІ ЧАТ-БОТИ СБУ, ГУР ТА МІНЦИФРИ.* https://zn.ua/ukr/UKRAINE/telegram-rozblokuvav-ofitsijni-chat-boti-sbu-hur-ta-mintsifri.html/

14. *Політика конфіденційності Telegram.* (n. d.). https://telegram.org/privacy/ua
15. Ярова, М. (n. d.). *Усе, що можна дізнатися про вас у Telegram-ботах.* https://ain.ua/2023/03/03/use-shho-mozhna-diznatysya-pro-vas-u-telegram-botah/
16. Ївженко, Д. (n. d.). *Засновник Signal заявив, що навіть Facebook Messenger більш захищений ніж Telegram.* https://ain.ua/2021/12/28/zasnovnyk-signal-facebook-messenger-telegram/
17. Токар, Н. (n. d.). *8 доказів небезпеки одного з найуспішніших російських проєктів Telegram.* https://cripo.com.ua/vojna-s-rf/8-dokaziv-nebezpeky-odnogo-z-najuspishnishyh-rosijskyh-proyektiv-telegram/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Valentyna Zaporozhets
Student, Department of Information Security
Lviv Polytechnic National University, Information Security Department, Lviv, Ukraine
ORCID ID: 0009-0006-6918-7784
valentyna.zaporozhets.kb.2022@lpnu.ua

Ivan Opirskyy
Doctor of Technical Sciences, Professor,
Head of the Department of Information Security
Lviv Polytechnic National University, Information Security Department, Lviv, Ukraine
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

THE DANGER OF USING TELEGRAM AND ITS IMPACT ON UKRAINIAN SOCIETY

Abstract. The article is devoted to an overview of the multi-platform messenger Telegram, a study of its use and an overview of the reasons for its great popularity in Ukraine, and the provision of detailed methodological recommendations for ensuring the security of users' personal data in accordance with the latest cybersecurity practices. This article highlights the main problems of the popular messenger, starting with certain clauses of the privacy policy of this application; using examples, it shows how users' confidential information is collected in the modern digital environment through various chatbots and information channels; shows the dangerous impact of such channels on the formation of political opinion of Ukrainian society; reviews Telegram's own encryption algorithm MTProto for regular chats and secret chats with end-to-end encryption and identifies the problems associated with the use of the application. The article focuses on the importance of protecting confidential data of Telegram account holders. The storage and processing of this type of data requires a high level of security, since their unauthorized leakage or breach of integrity can lead to the theft of other types of information, as well as to the loss of user trust. The article investigates the main problems faced by users of the Telegram application in the field of cybersecurity and proposes effective approaches to their solution through secure manual configuration of Telegram, as well as recommendations on the correct handling of users' personal data to preserve their confidentiality and integrity. This approach allows to adapt to the ever-changing environment of cyber threats and increases the level of protection of personal data of individuals. Thus, by analyzing the above aspects, the article makes readers aware of the dangers of using the Telegram application during a full-scale war in Ukraine, helps to understand the current challenges in the field of cybersecurity, and provides detailed recommendations for countering these challenges.

Keywords: Telegram; user data; chatbots; information channels; information theft; MTProto; secure configuration.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. The Next Web. (n. d.). *Telegram introduces end-to-end encrypted video calls.* https://thenextweb.com/news/telegram-introduces-end-to-end-encrypted-video-calls/
2. *Article 2 of the Law of Ukraine "On Personal Data Protection".* (n. d.). https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Garkava, T., Moneva, A., & Leukfeldt, E. R. (2024). Stolen data markets on Telegram: a crime script analysis and situational crime prevention measures. *Trends Organ Crim.* https://doi.org/10.1007/s12117-024-09532-6
4. Theisen, W., et al. (2024). An Avalanche of Images on Telegram Preceded Russia's Full-Scale Invasion of Ukraine. *arXiv.* https://doi.org/10.48550/arXiv.2402.14947

5. Komiljonov, J. (2024). How Safe Telegram Is to Keep Personal Data and Conversations. *EUROPEAN JOURNAL OF BUSINESS STARTUPS AND OPEN SOCIETY, 4(2),* 54–57.
6. *The Evolution of Telegram.* (n. d.). https://telegram.org/evolution#october-2013
7. Witman, E. (2021). *How to make a Telegram account and start using the popular group chatting app. Business Insider. https://www.businessinsider.com/guides/tech/how-to-make-a-telegram-account*
8. *List of Telegram applications.* (n. d.). https://telegram.org
9. *Durov's Channel*. (n. d.). https://t.me/durov/148
10. Bunyak, V. (2024). *Durov in an interview with the Financial Times: The number of Telegram users reached 900 million in February 2024.* https://ms.detector.media/trendi/post/34401/2024-03-11-durov-v-intervyu-financial-times-kilkist-korystuvachiv-telegramu-syagnula-900-milyoniv-u-lyutomu-2024-roku/
11. *Most Popular Messaging Apps by Country — Similarweb.* (n. d.). https://www.similarweb.com/blog/research/market-research/worldwide-messaging-apps
12. Kudina, M. (n. d.). *Telegram: why it is so popular among Ukrainians and what dangers it hides.* https://netfreedom.org.ua/article/telegram-chomu-vin-takij-populyarnij-sered-ukrayinciv-ta-yaki-nebezpeki-prihovuye
13. Moskalenko, Y. (n. d.). *TELEGRAM UNBROKE OFFICIAL CHATBOTS OF SBU, GUR and MINISTRY*. https://zn.ua/ukr/UKRAINE/telegram-rozblokuvav-ofitsijni-chat-boti-sbu-hur-ta-mintsifri.html/
14. *Telegram Privacy Policy.* (n. d.). https://telegram.org/privacy/ua
15. Yarova, M. (n. d.). *Everything Telegram bots can learn about you.* https://ain.ua/2023/03/03/use-shho-mozhna-diznatysya-pro-vas-u-telegram-botah/
16. Yivzhenko, D. (n. d.). *Signal's founder said that even Facebook Messenger is more secure than Telegram.* https://ain.ua/2021/12/28/zasnovnyk-signal-facebook-messenger-telegram/
17. Tokar, N. (n. d.). *8 proofs of the danger of one of Russia's most successful projects, Telegram.* https://cripo.com.ua/vojna-s-rf/8-dokaziv-nebezpeky-odnogo-z-najuspishnishyh-rosijskyh-proyektiv-telegram/