# СЕКЦІЯ 2. ПРАВОВІ АСПЕКТИ БЕЗПЕКИ Й ЗАХИСТУ ІНФОРМАЦІЇ У ЦИФРОВОМУ ПРОСТОРІ В ПОВОЄННИЙ ЧАС

DOI https://doi.org/10.36059/978-966-397-389-0-3

## ПРАВОВІ АСПЕКТИ ВИКОРИСТАННЯ ТА РЕГУЛЮВАННЯ МЕСЕНДЖЕРІВ

**Дрижакова Діна Юріївна**
*аспірантка кафедри кримінально-правової політики та кримінального права*
*Київський національний університет імені Тараса Шевченка*
*м. Київ, Україна*

Хто володіє інформацією, той володіє світом.
*Вінстон Черчіль*

Актуальність теми: на сьогодні з розвитком цифрових технологій та цифровізації набуває актуальності захист інформації, що передається за допомогою месенджерів. Месенджери стали частиною суспільного життя мільйонів людей і використовуються не лише в якості інструменту для спілкування, а й для маркетингу, бізнесу та навчання. Вони є у кожного користувача смартфона, а для передачі даних використовують цифрові канали зв'язку.

Метою дослідження: є пошук шляхів правового захисту використання месенджерів та інформації, що ними передається.

Виклад основного матеріалу: Інформація у сучасному світі являє собою стратегічний ресурс. Її спотворення, перехоплення або блокування може призвести до серйозних наслідків, а в умовах стрімких світових змін набувають актуальності існуючі та формуються нові загрози національній безпеці України.

Важливою складовою захищеності та безпеки інформації є етап передачі інформації цифровими каналами зв'язку, адже саме на цьому етапі існують ризики перехоплення даних. Під час перехоплення пакетів даних, які прямують незахищеними (або частково захищеними) каналами зв'язку, створюються передумови для спотворення чи блокування інформації, а також для перехоплення персональних, конфіденційних та/або даних з обмеженим доступом [1].

В умовах повномасштабного вторгнення використання об’єктивно захищеного месенджеру для обміну даними між військовослужбовцями ЗСУ набуває все більшої актуальності.

На сьогодні шляхом робочого спілкування військовослужбовців між собою поширюються наступні дані:

– персональні ідентифікаційні дані;

– інформація щодо проходження військової служби (підрозділ, звання, завдання, поточні задачі, дані про дислокацію та ротацію тощо);

– дані для службового користування або ж дані з обмеженим доступом.

Слід також звернути увагу на захищеність самих месенджерів, де військові зберігають дані, на їхніх розпорядників (розробників), а також на різноманітні програмно-апаратні вразливості.

Слід враховувати, що встановлюючи будь-який із месенджерів ми погоджуємось із правилами користування, які встановлені розробником.

Доволі часто з цими правилами просто погоджуємось, не читаючи.

Слід розглянути декілька найбільш вжваних в Україні месенджерів.

WhatsApp – пропрієтарний месенджер для смартфонів. Він дозволяє пересилати текстові повідомлення, зображення, відео та аудіо. Клієнт працює на платформах Android, BlackBerry OS, BlackBerry 10, iOS, Series 40, Symbian (S60) і Windows Phone. Має десктоп версії з травня 2016 року. WhatsApp – це одна з найбільш використовуваних служб обміну повідомленнями у світі, але створює проблеми щодо використання даних користувачів. Слід зазначити, що він гарантує наскрізне шифрування для всіх обмінів, але певні дані можуть бути передані іншим об’єктам Facebook, наприклад номер телефону, дані транзакцій або інформація про взаємодію користувача.

Відомо, що додаток WhatsApp зберігає повідомлення на телефоні, а також на хмарному сервері iCLoud, з використанням протоколу підтримки шифрованих групових чатів. При цьому зміст розмов не зберігається, але номера, на які ви дзвонили, модель телефону, IP-адреса і версія ОС залишаються в базі. З процесом реформування месенджеру під проєкт Meta змінюється політика конфіденційності, проте не вся.

З огляду на простоту процедури ідентифікації особи за номером мобільного телефону та його прив’язку до WhatsApp країною агресором, можливо, здійснюються дезінформаційні акції впливу на громадян України.

У цьому році хакери через Signal намагалися атакувати комп'ютери українських військових.

Кіберзлочинці, видаючи себе за колег військовослужбовців, надсилали XLS-документ, прикрашений як звіт, з проханням допомогти в його заповненні. Однак цей документ містив шкідливий код, який при запуску завантажував і виконував на комп'ютері жертви шкідливу програму COOKBOX [2].

Росіяни збільшують кількість кібератак з метою шпигунства.

Такі російські групи, як Gamaredon, GREF і SturgeonPhisher, **націлювалися на користувачів Telegram** з метою викрадення інформації або пов'язаних метаданих. Тоді як Sandworm, ще одна група з росії, теж активно використовувала цей месенджер для реклами своїх дій кіберсаботажу. Крім цього, група поширювала нові версії уже відомих загроз та нові програми для **знищення даних, націлені на державні організації, приватні компанії та медіаорганізацію** в Україні [3].

Розробником кожного месенджера в більшості випадків вбудовано в програму бот, який в певній формі збирає та надсилає дані користувачів розробникам.

З'явилося положення, що Telegram може передавати спецслужбам IP-адреси та номер телефону користувачів, яких підозрюють в тероризмі. Для цього правоохоронцям потрібно надіслати запит адміністрації месенджера та додати до нього рішення суду [4].

Так, у Швейцарії Закон 2016 року про розвідувальну службу, надав можливість національним службам у сфері кіберрозвідки для тотального шпигунства за власними громадянами в Інтернеті.

Прийняття Закону України «Про електронні комунікації» [5] певним чином врегульовує господарсько-технічні питання, однак далеко не вичерпує питання загальної організації електронної форми публічних комунікацій. Конкретною ілюстрацією даної проблеми може слугувати, без перебільшення, кризова ситуація, що склалась навколо процесуальних комунікацій судів з учасниками відповідних справ щодо надсилання судових повідомлень, викликів, і особливо, рішень [6].

Йдеться, зокрема, про надсилання учасникам справи судових повідомлень, викликів, а також рішень за допомогою інтернет-месенджерів. Фактично маються на увазі додатки типу Viber, WhatsApp.

Слід зауважити, що безпосереднє використання для судових повідомлень інтернет-месенджерів процесуальним законодавством не передбачено. Це можна зробити опосередковано, через мобільний зв'язок, можливість використання якого таким законодавством передбачено. Так, відповідно до ст. 120 Господарського процесуального кодексу суд може застосувати мобільний зв'язок для надсилання повідомлення або у випадках термінової необхідності

(ч. 6), або за наявності відповідної письмової заяви учасника справи (ч. 9) [7]. Умова фіксації повідомлення при цьому є обов'язковою.

Висновок: На сьогодні відповідно до ч. 2 ст. 19 Закону України «Про електронні комунікації» надання електронних комунікаційних послуг на території України є виключним правом юридичних осіб та фізичних осіб – підприємців, зареєстрованих відповідно до законодавства (резиденти України) [5]. Однак процесуальне законодавство вимагає наразі використання месенджерів типу Viber, WhatsApp. Цифровізація українського суспільна у період тим більше воєнного стану вимагає внесення змін до законодавства про електронні комунікації щодо визначення правового становища месенджерів та результатів інформації, що ними передається. Існує необхідність в укладенні додаткових міжнародних угод із країнами-розробниками месенджерів щодо доступу українських правоохоронців до інформації з обмеженим доступом месенджерів, так і щодо підвищення ступеня захищеності інформації, що передається.

**Література:**

1. Використання месенджерів як елементів цифрової розвідки: проблематика та шляхи вирішення. URL: https://intelmag.com/digitalization/17454-vykorystannya-mesendzheriv-yak-elementiv-czyfrovoyi-rozvidky-problematyka-ta-shlyahy-vyrishennya/

2. Хакери через Signal намагалися атакувати комп'ютери українських військових. URL: https://sud.ua/uk/news/ukraine/294204-khakery-cherez-signal-pytalis-atakovat-kompyutery-ukrainskikh-voennykh

3. Від диверсій до шпигунства: як змінилися кібератаки російських хакерів в Україні. URL: https://www.eset.com/ua/about/newsroom/press-releases/malware/vid-dyversiy-do-shpyhunstva-yak-zminylysya-kiberataky-rosiyskykh-khakeriv-v-ukrayini/

4. Telegram передаватиме спецслужбам дані про підозрюваних у тероризмі. URL: https://www.bbc.com/ukrainian/news-45334630

5. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. *Офіційний веб-портал ВРУ.* URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

6. Ясинська М. Нові проблеми належного повідомлення. *Юридична практика*. № 17–18(1218–1219) від 04.05.2021. URL: https://pravo.ua/articles/informatsiine-zabezpechennia

7. Господарський процесуальний кодекс України: від 6 листопада 1991р. № 1798XII. *Офіційний портал ВРУ*. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text