***УДК:342.7***
***https://doi.org/10.32703/2663-6352/2026-1-19-179-190***
***https://orcid.org/0009-0000-4442-0275***
***Гриценко П. В.,***
*аспірант Національної академії*
*Служби безпеки України*
*м. Київ, Україна*

# TELEGRAM ЯК ІНСТРУМЕНТ ПОШУКУ ТА ЗБОРУ ІНФОРМАЦІЇ ДЛЯ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ: ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ, РИЗИКИ ТА НАПРЯМИ ПРАВОВОГО РЕАГУВАННЯ

***Анотація.*** *У статті досліджено використання месенджера Telegram як конвергентного цифрового середовища, що одночасно виконує функції оперативного інформування, координації, краудсорсингу даних та платформи для OSINT-спостережень, водночас формуючи суттєві кібербезпекові та контррозвідувальні ризики для сектору безпеки і оборони. Визначено ключові моделі застосування Telegram в умовах повномасштабної агресії рф проти України: збір розвідданих від населення через офіційні боти; моніторинг повітряних загроз; гуманітарний пошук і волонтерська логістика; аналітичні OSINT-практики. Показано, що з 2024–2026 років паралельно еволюціонувала протилежна, ворожа функція платформи – вербування «одноразових агентів» за логікою «gig-економу саботажу» (диверсії, підпали, розвідка, підготовка терористичних актів), з використанням ботів, анонімізації та криптовалютних розрахунків. Обґрунтовано, що державна політика має поєднувати: (1) нормативне обмеження використання Telegram на службових пристроях; (2) протоколи безпечного застосування для дозволених службових задач; (3) системну інформаційну протидію вербуванню; (4) узгоджені процедури цифрової криміналістики й доказування у кримінальному провадженні.*

***Ключові слова:*** *Telegram, сектор безпеки, кібербезпека, OSINT; краудсорсинг, вербування, диверсійна діяльність, «одноразові агенти».*

# HRYTSENKO P. TELEGRAM AS A TOOL FOR SEARCHING AND COLLECTING INFORMATION FOR THE SECURITY AND DEFENSE SECTOR OF UKRAINE: FUNCTIONAL CAPABILITIES, RISKS AND DIRECTIONS OF LEGAL RESPONSE

***Abstract.*** *The article explores the use of the Telegram messenger as a convergent digital environment that integrates the functions of operational information, coordination of actions, crowdsourcing of data and a platform for OSINT observations. It is substantiated that in the conditions of the full-scale aggression of the Russian Federation against Ukraine, Telegram has transformed into an important tool for ensuring communication between state institutions, security and defense sector entities and civil society. It is shown that due to the high level of accessibility, speed of information dissemination and the possibilities of anonymous interaction, the platform has become widely used in the field of responding to military threats. At the same time, it is established that the above characteristics lead to the emergence of significant cybersecurity and counterintelligence risks associated with potential leaks of sensitive information, the lack of proper control over communication channels, the use of anonymous accounts and the difficulty of identifying interaction subjects. It is emphasized that such risks are of particular relevance in the context of hybrid warfare and information confrontation.*

*Key models of Telegram use in the context of full-scale aggression of the Russian Federation against Ukraine have been identified, including: collection of intelligence data from the population*

*through official chatbots; monitoring of air and missile threats in real time; organization of humanitarian search and coordination of volunteer logistics; implementation of analytical OSINT practices and dissemination of verified information. It has been proven that the use of these tools contributes to increasing the efficiency of management decisions and strengthening interaction between the state and society. At the same time, the transformation of Telegram into an environment for the implementation of illegal activities, which gained particular development in 2024–2026, has been analyzed. It has been established that the platform is used to recruit so-called "disposable agents" according to the "gig-economy sabotage" model, which involves the performance of individual criminal tasks (sabotage, arson, collection of intelligence information, preparation of terrorist acts) for a reward. The main mechanisms of such activity are revealed, in particular the use of anonymous channels, automated bots, encryption tools and cryptocurrency calculations, which complicates their detection and documentation.*

***Key words**: Telegram; security sector; cybersecurity; OSINT (Open-Source Intelligence); crowdsourcing; recruitment; sabotage activity; "disposable agents".*

**Вступ**. Війна змінила не лише карту загроз, а й архітектуру інформаційного простору. Те, що ще вчора сприймалося як зручний месенджер для побутових комунікацій, сьогодні стало фактичним «нервовим вузлом» оперативних повідомлень, сигналів тривоги, свідчень очевидців і цифрових слідів, що мають безпосереднє значення для національної безпеки. У цьому вимірі Telegram перетворився на явище, яке важко оцінити однозначно: він одночасно дає швидкість, охоплення й ефект мережі, але так само акумулює ризики від маніпуляції та дезінформації до витоку чутливих даних і ворожого використання каналів та ботів.

Для сектору безпеки і оборони України Telegram став інструментом, через який у стислий час може «піднятися» інформація знизу – від громадянина, волонтера, очевидця – до інституцій, здатних реагувати. Він створює середовище для пошуку та збору відомостей у реальному часі, допомагає структурувати повідомлення, організовувати взаємодію, підтримувати публічні комунікації та мобілізацію суспільства. Однак та сама швидкість і відкритість, що працюють на користь, створюють і системну вразливість: противник використовує платформу для вербування, координації саботажу, формування «сірих» мереж інформаторів, підміни офіційних каналів, а також для збирання метаданих, які здатні перетворити невинну публікацію на джерело розвідданих.

У такій ситуації правовий вимір стає визначальним. Питання вже не зводиться до індивідуальної цифрової обережності користувача чи загальних рекомендацій з кібергігієни. Йдеться про потребу системного правового реагування, яке має одночасно зберегти корисні функції Telegram як інструменту пошуку та збору інформації для публічних потреб і водночас мінімізувати шкоду, встановивши зрозумілі межі допустимого використання. Це передбачає чітке розмежування дозволених і заборонених сценаріїв, формалізацію правил службового користування, критерії оцінки ризиків для різних категорій інформації, а також належні процедури фіксації, верифікації та доказування цифрових відомостей у правозастосуванні.

Саме тому дослідження Telegram як інструменту пошуку та збору інформації для сектору безпеки і оборони України виходить за межі технологічної тематики й набуває характеру комплексної проблеми публічного права та національної безпеки. У центрі уваги функціональні можливості платформи, які реально використовуються в умовах війни; спектр ризиків, що супроводжують такі практики; а також напрями правового реагування, здатні забезпечити баланс між оперативністю інформаційного обміну і вимогами безпеки, правової визначеності та відповідальності.

**Постановка проблеми**. В умовах повномасштабного вторгнення рф у лютому 2022 року цифрові мережі стали середовищем мобілізації суспільства, оперативних комунікацій та організації взаємодії між громадянами і державою. У цьому контексті Telegram набув подвійної природи: з одного боку – швидкісного каналу пошуку/поширення оперативної інформації, з іншого – джерела критичних ризиків кібербезпеки та контррозвідки для сектору безпеки і оборони.

Станом на лютий 2026 року Telegram постає як особливе явище у контексті війни: він водночас виконує роль провідного каналу отримання оперативної інформації та формує суттєві ризики для кібербезпеки. Для сектору оборони України цей месенджер використовується як багатофункціональна платформа пошуку й акумулювання даних, однак його застосування має здійснюватися в межах жорстко визначених обмежень. У результаті Telegram зберігає статус одного з ключових, хоча й суперечливих, інструментів інформаційного пошуку та збору відомостей для потреб оборонного сектору.

Актуальність такого підходу зумовлена тим, що Telegram фактично перетворився на інфраструктуру інформаційного обміну, яка за швидкістю поширення та обробки повідомлень випереджає традиційні організаційні механізми державного управління. Відтак він потребує правового й організаційного інтегрування у загальний режим безпеки, що передбачає чітке визначення дозволених і заборонених сценаріїв використання, запровадження процедур мінімізації ризиків і шкоди, а також унормування підходів до фіксації та доказування інформації, отриманої через цифрові канали.

Мета статті полягає у визначенні функціональних моделей використання Telegram для пошуку й збору інформації у секторі безпеки і оборони України та окресленні ризиків і напрямів правового реагування.

Наукова новизна та практичне значення дослідження. Наукова новизна дослідження полягає в тому, що Telegram концептуалізовано не як окремий технічний сервіс, а як соціотехнічну інфраструктуру гібридної агресії з подвійним режимом функціонування у секторі безпеки і оборони: корисним (краудсорсинг, OSINT, моніторинг, гуманітарні сценарії) та ворожо-деструктивним (вербування «одноразових агентів», «gig-economy саботажу», підміна автентичності, криптофінансування). Уперше у межах єдиного науково-правового викладу запропоновано рамку правового реагування, що поєднує адміністративно-правові обмеження службового використання з комплаєнс-процедурами дозволених сценаріїв, кримінально-правовими запобіжниками для чутливих категорій відомостей та процедурними підходами до верифікації й цифрового доказування. Додатково обґрунтовано, що OSINT-практики в Telegram мають оцінюватися за критеріями правової допустимості (фактичний зміст дій, контекст воєнного стану, чутливість даних, наявність санкціонованих каналів), що дозволяє практично відмежовувати законне інформаційне реагування від дій, здатних прямо або опосередковано сприяти противнику.

Практичне значення отриманих результатів полягає в тому, що сформульовані у статті підходи можуть бути використані для удосконалення профілактичної діяльності СБУ та інших уповноважених суб'єктів у сфері інформаційної безпеки, зокрема при розробленні внутрішніх регламентів безпечного використання месенджерів, процедур верифікації повідомлень, стандартів належної обачності для персоналу та підходів до документування цифрових відомостей. Запропонована рамка також придатна для практики органів державної влади у частині балансування комунікаційної ефективності (оперативні сповіщення, краудсорсинг) із вимогами кібербезпеки та контррозвідки, а в науковому вимірі для подальшого розвитку адміністративно-правової доктрини національної безпеки щодо правових режимів використання цифрових платформ в умовах воєнного стану.

Виклад основного матеріалу. Із початком повномасштабного вторгнення російської федерації на територію України у лютому 2022 року цифрові мережі та платформи комунікації набули статусу активного середовища для оборони держави, суспільної мобілізації та організації взаємодії між громадянами, волонтерськими ініціативами й державними інституціями. У цих умовах Telegram поступово трансформувався з інструмента повсякденного спілкування у фактичну інфраструктуру швидкісного інформаційного обміну, яка забезпечує як пошук, так і збір відомостей, що мають значення для потреб безпеки й оборони. Станом на лютий 2026 року Telegram постає як унікальний феномен війни: він одночасно виконує функцію одного з ключових джерел оперативних повідомлень і водночас є середовищем, у межах якого реалізуються інформаційні, розвідувальні та диверсійні практики противника. Така подвійність зумовлює необхідність розглядати Telegram не лише крізь призму технічних заходів кіберзахисту, а й у площині правового регулювання, що має визначати допустимі сценарії використання, межі обігу чутливої інформації та механізми мінімізації шкоди. Для сектору безпеки і оборони України Telegram функціонує як багатофункціональний інструмент пошуку та акумулювання даних, однак його застосування об'єктивно потребує суворих обмежень і процедурної дисципліни, що, своєю чергою, вимагає послідовного аналізу як фактичних практик використання месенджера, так і правових меж їх допустимості, процедур фіксації та верифікації інформації, а також наслідків її неправомірного поширення.

За висновками українських та міжнародних дослідницьких і аналітичних центрів Telegram фактично перетворився на один із ключових «цифрових фронтів» війни проти України. Актуальність проблематики посилюється тим, що, попри ухвалені державними органами рішення щодо заборони або суттєвого обмеження використання Telegram на службових пристроях [8] у секторі безпеки і оборони, цей месенджер продовжує залишатися одним із наймасовіших каналів отримання новин для громадян, а отже формує ризикове інформаційне середовище, у якому деструктивні впливи, маніпулятивні повідомлення та ворожі інформаційні операції здатні поширюватися з високою швидкістю та поза належними механізмами контролю [13]. Відповіддю держави на цю структурну суперечність стало інституціоналізоване обмеження службового використання месенджера та формування підвищених стандартів інформаційної безпеки для суб'єктів сектору безпеки і оборони.

Станом на 2026 рік, відповідно до рішень НКЦК, використання Telegram на службових пристроях військовослужбовців і державних службовців підлягає суворому обмеженню у зв'язку з ризиком несанкціонованого доступу до даних з боку спецслужб рф. У практичному вимірі це означає жорстко регламентований режим застосування месенджера в оборонному секторі: передусім – заборону використання на службових комп'ютерах і смартфонах, запроваджену рішенням НКЦК (РНБО) у вересні 2024 року; підвищений ризик компрометації геолокації та позицій у разі використання поблизу лінії фронту через метадані та характер мережевої активності; а також системну загрозу доступу російських спецслужб до персональних даних і комунікацій користувачів, включно з повідомленнями, які були видалені, на що неодноразово звертали увагу керівники українських розвідувальних органів.

У вітчизняному науковому дискурсі проблематика Telegram у контексті війни та безпеки розкривається через суміжні дослідницькі напрями, які у сукупності формують рамку для аналізу функціональних можливостей платформи, спектра ризиків і логіки правового реагування [1; 3–5; 7]. Зокрема, у статті Н. Баловсяк «Комунікація державних органів України у телеграмі в умовах ризиків та обмежень» Telegram осмислюється як оперативна інфраструктура державного інформування в умовах воєнного часу, що водночас актуалізує питання регламентованих сценаріїв використання, комплаєнс-процедур та розмежування службових і позаслужбових практик комунікації [1]. Понятійно-типологічну основу для розуміння Telegram як

багаторівневого середовища з різними режимами довіри й автентичності забезпечує дослідження «Анонімні та офіційні Telegram-канали в Україні: аналіз популярності під час гібридної війни», яке дозволяє пов'язати структуру українського сегмента платформи з проблемою верифікації інформації та її правової оцінки [2]. Кібербезпековий вимір проблематики розкрито у праці В. Запорожця «Небезпека використання Telegram та його вплив на українське суспільство», де акцентовано увагу на ризиках компрометації даних, витоків інформації та наслідках для довіри користувачів, що може бути використано для юридичного обґрунтування підвищених вимог до захисту інформації у публічному секторі [3]. Додатковий методологічний горизонт формують праці з OSINT, зокрема дослідження В. Івкової «OSINT-технології як загроза кібербезпеці держави», у якому доводиться, що відкриті цифрові джерела здатні перетворюватися на інструмент збору чутливих відомостей для атак, а отже цифровий пошук інформації має правові межі та безпекові наслідки[4]; подібну логіку підтримують і матеріали круглого столу «Роль OSINT-досліджень у підвищенні рівня національної безпеки України», де OSINT осмислюється як інструмент національної безпеки за умови дотримання методичних стандартів і правових застережень [5]. Як підтвердження того, що Telegram аналізується також у межах академічних досліджень інформаційної поведінки в кризових умовах, можна залучати роботу Т. Гордієнко «The use of digital platforms in a crisis: the case of Telegram and the impact of war on media consumption (case of Ukraine after 2022)», яка розкриває моделі споживання інформації через Telegram у війні та механізми формування довіри до контенту [6]. Водночас інституційний контекст державної політики та аргументації обмежень відображено в аналітичному матеріалі Національного інституту стратегічних досліджень «Використання Telegram: доступ до інформації vs загроза нацбезпеці», який окреслює дилему балансу між комунікаційною ефективністю та вимогами безпеки [7]. У сукупності зазначені напрацювання дозволяють обґрунтовано перейти до аналізу конкретних моделей використання Telegram як інструменту пошуку та збору інформації для сектору безпеки і оборони, одночасно розкриваючи правові межі допустимого використання, ризики неправомірного поширення чутливих відомостей і напрями правового реагування, спрямовані на мінімізацію шкоди та забезпечення належної доказовості цифрових даних [1–7].

Подальший аналіз вибудовується навколо типових практик використання Telegram у воєнний час як інструменту пошуку та акумулювання інформації: структурованого краудсорсингу через боти і канали зворотного зв'язку, моніторингу загроз та оперативних повідомлень, OSINT-практик роботи з відкритими цифровими джерелами, а також гуманітарних і логістичних сценаріїв (пошук зниклих, координація волонтерської допомоги, комунікація щодо ресурсів). Така побудова дозволяє в кожній із зазначених моделей окремо показати, які саме ризики виникають унаслідок використання месенджера, і які правові механізми є релевантними для їх нейтралізації від режиму службового користування та захисту даних до вимог верифікації й процесуальної придатності цифрових відомостей.

Для науково-правового викладу тут принциповим є висновок про те, що режим використання месенджера у публічній службі має характер адміністративно-правового обмеження, спрямованого на захист публічного інтересу (безпеки та оборони), а його недотримання потенційно тягне дисциплінарні та інші юридичні наслідки залежно від наслідків витоку, статусу інформації та кола суб'єктів. Водночас сам факт обмеження не усуває реальності використання Telegram у приватному секторі й волонтерському середовищі, що потребує комплексної моделі комплаєнсу: поєднання організаційних заборон (на службових пристроях), технічних налаштувань безпеки (двофакторна автентифікація, обмеження видимості номера, керування вбудованим браузером) та правового інструктажу щодо недопустимих категорій контенту

Практична цінність Telegram для оборонного сектору розкривається передусім через інструменти структурованого збору інформації від населення, де «пошук» працює у зворотному напрямку: не користувач шукає дані, а уповноважені органи отримують стандартизовані повідомлення, придатні для оперативної перевірки та використання. У цій логіці боти державних органів перетворюють приватну ініціативу громадян на керований потік даних, знижуючи транзакційні витрати на первинний збір відомостей і водночас підвищуючи вимоги до правового режиму таких повідомлень (ідентифікації/автентифікації, захисту персональних даних, цільового використання інформації, збереження та доступу).

Саме тому в українській практиці сформовано цілу мережу офіційних ботів, функціонально зорієнтованих на фіксацію техніки, окупантів і колаборантів, а також на конфіденційне передавання розвідувально значущих відомостей, що відображає інституціоналізацію "громадянського сенсингу" як допоміжного механізму оборони. Ці боти, залучаючи громадян до повідомлень про загрози, фактично розширюють спостережний контур держави й дають змогу перетворювати поодинокі сигнали на структуровані дані, придатні для подальшої верифікації та реагування.

• @evorog_bot (єВорог) [10]: пошук і фіксація техніки, окупантів та колаборантів через авторизацію в «Дії».

• @stop_russian_war_bot [11]: офіційний бот СБУ для збору даних про переміщення ворога.

• @gur_official_bot: головний бот розвідки (ГУР) для конфіденційної передачі стратегічно важливої інформації.

У юридичному вимірі така практика має оцінюватися крізь призму допустимості обробки даних у сфері національної безпеки, меж службового використання інформації, належного інформування громадян про наслідки поширення відомостей і гарантій невтручання у приватність понад необхідне. Окремого значення набуває принцип правової визначеності: користувачі повинні розуміти, які відомості дозволено передавати, у які канали, в якій формі, та які категорії даних можуть утворювати склад правопорушення у разі їх поширення поза визначеними процедурами.

Другий вимір оборонної корисності Telegram пов'язаний із моніторингом повітряних загроз та OSINT-практиками, у межах яких швидкість обігу повідомлень нерідко випереджає традиційні інформаційні контури та офіційні комунікаційні цикли. У цьому сегменті Telegram фактично виконує функцію високодинамічного середовища раннього попередження: через спеціалізовані моніторингові канали, що спираються на мережі спостерігачів і технічні засоби, у режимі, наближеному до реального часу, акумулюються та поширюються повідомлення про пуски ракет і переміщення безпілотних літальних апаратів; як приклади таких інформаційних вузлів у публічному просторі часто згадуються канали «Николаевский Ванек» та «monitor». Паралельно Telegram функціонує як інфраструктура для OSINT-аналізу, оскільки саме в цьому середовищі дослідницькі спільноти оперативно відшукують візуальні докази (фото- та відеоматеріали) з тимчасово окупованих територій або з російських публічних ресурсів і здійснюють подальшу геолокацію техніки та ідентифікацію підрозділів РФ. Таким чином, Telegram поєднує два взаємодоповнювальні режими інформаційної роботи – оперативне моніторингове сповіщення та аналітичне опрацювання відкритих джерел, що підсилює його значення для оборонних потреб, але водночас загострює вимоги до верифікації повідомлень і дотримання правових меж поширення чутливої інформації.

Водночас саме в цьому сегменті постає ключова правова дилема: потреба оперативного інформування населення про повітряну загрозу не може слугувати виправданням поширення відомостей, здатних завдати шкоди обороні, розкрити дислокацію сил або створити передумови для коригування ворожих ударів. З огляду на це у науково-правовому аналізі доцільно

розмежовувати повідомлення «про загрозу» (які спрямовані на підвищення безпеки населення та мають превентивний характер) і повідомлення «про військові об'єкти, переміщення підрозділів, наслідки уражень» (які можуть створювати ризик розкриття чутливої інформації та підпадати під кримінально-правові заборони). Практика воєнного часу підтверджує, що навіть зовні «технічні» або, на перший погляд, низькорівневі дії, зокрема фото- чи відеофіксація інфраструктурних об'єктів, переміщень, результатів обстрілів можуть розглядатися як суспільно небезпечні за критерієм їх потенційної розвідувальної цінності для противника, а отже породжують ризик кримінально-правової відповідальності за обставин, визначених законом.

У цьому контексті насамперед слід мати на увазі статтю 114-2 КК України, яка встановлює відповідальність за несанкціоноване поширення інформації про переміщення, рух або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань в умовах воєнного стану; санкція цієї норми передбачає покарання у вигляді позбавлення волі на строк від 3 до 12 років. Окремо, за наявності ознак умисної діяльності в інтересах держави-агресора, зокрема якщо встановлюється, що особа діяла «на замовлення» або у взаємодії з представниками (кураторами) спецслужб РФ, правова оцінка може виходити за межі статті 114-2 і набувати кваліфікації за статтею 111 КК України (державна зрада), за якою передбачено покарання у вигляді позбавлення волі на строк 15 років або довічного позбавлення волі з конфіскацією майна. Така постановка питання дозволяє інтегрувати у текст статті принциповий висновок: OSINT як метод не перебуває «поза правом», а його допустимість визначається не назвою практики, а об'єктивним змістом дій, контекстом воєнного стану, характером і чутливістю поширюваних відомостей, а також наявністю або відсутністю санкціонованих каналів взаємодії з уповноваженими державними органами.

Отже, застосування OSINT-практик у середовищі Telegram має оцінюватися в категоріях правової допустимості: вирішальними є не назва чи «метод», а фактичний зміст дій, воєнно-правовий контекст, чутливість поширюваних відомостей та наявність належних, санкціонованих каналів взаємодії з уповноваженими органами.

Третій вимір використання Telegram у секторі безпеки і оборони стосується гуманітарного пошуку та кадрово-логістичних комунікацій. Спеціалізовані боти від Координаційного штабу допомагають родичам шукати інформацію про військовополонених або зниклих безвісти. Крім того, пошук комплектуючих для дронів, специфічного обладнання чи транспорту відбувається через закриті та відкриті групи волонтерів і виробників. Для перевірки інформації про діяльність СБУ в Telegram, списки ворожих ресурсів та офіційні обмеження, варто звертатися виключно до першоджерел.

Юридично зазначені практики потребують підвищеної обережності, оскільки цифрове середовище Telegram об'єктивно створює ризики шахрайства, компрометації персональних даних, проникнення агентури у тематичні спільноти та підміни офіційних каналів комунікації. За таких умов нормативно-організаційний акцент має бути зміщений у бік пріоритету першоджерел і верифікованих ресурсів, а також забезпечення процедурної дисципліни в обігу інформації: перевірки повідомлень перед їх використанням або поширенням, мінімізації персональних даних у відкритих чатах, використання виключно офіційних ботів і каналів із підтвердженою автентичністю, а також фіксації підозрілих контактів і повідомлень для подальшого реагування уповноваженими суб'єктами. У цьому зв'язку як орієнтир для верифікації та отримання офіційних роз'яснень доцільно використовувати державні інформаційні ресурси, зокрема: ssu.gov.ua – офіційний сайт Служби безпеки України, на якому публікуються повідомлення про викриття агентурних мереж і застереження щодо інформаційної безпеки; cpd.gov.ua – сайт Центру протидії дезінформації при РНБО, де, зокрема, оприлюднюються матеріали щодо інформаційних операцій та ідентифікації пропагандистських ресурсів; rnbo.gov.ua – ресурс Ради національної

безпеки і оборони України, що містить рішення та інші документи, пов'язані з формуванням державної політики у сфері інформаційної безпеки, у тому числі щодо режимів використання цифрових платформ; gur.gov.ua – офіційний сайт Головного управління розвідки Міністерства оборони України, на якому розміщуються повідомлення про загрози та офіційні канали взаємодії.

Найбільш загрозливим у сучасній конфігурації Telegram-екосистеми є використання платформи противником для вербування «одноразових агентів» і реалізації тактики «диверсійного краудсорсингу», коли рекрутинг і керування виконавцями масштабуються через боти та мережі каналів, а виконавець часто не усвідомлює кінцевого замовника. У наведеному викладі простежується еволюція такого цифрового рекрутингу у 2024–2026 роках: відтворюється логіка «гіг-економіки» саботажу, окреслюються типові канали пошуку кандидатів у радикальних спільнотах, групах із працевлаштування та міграційних чатах, а також розкривається поетапна «воронка» втягування від «тестових» дрібних правопорушень до диверсій і терактів. Паралельно акцентується, що фінансування таких дій здебільшого здійснюється через криптовалюти, а механізми контролю над виконавцями можуть включати шантаж і використання підробленої легенди (false flag), коли вербувальники видають себе за українські структури.

Юридично окреслені вимоги до верифікації першоджерел, мінімізації персональних даних і використання лише автентичних офіційних каналів набувають особливої ваги в контексті ще одного явища воєнного часу – трансформації Telegram на інструмент не лише інформаційного обміну, а й організації злочинної діяльності, зокрема вербування та координації диверсій. У 2024–2025 роках російські спецслужби (насамперед структури, пов'язані з ГРУ та ФСБ) системно перейшли до тактики так званого «диверсійного краудсорсингу», коли залучення виконавців відбувається дистанційно, у масовому форматі та під «прикриттям» псевдоцивільних оголошень. У цій моделі Telegram виступає базовою платформою цифрового рекрутингу «одноразових агентів», а сам процес вербування набуває рис «гіг-економіки»: виконавцеві пропонується «підробіток», завдання дробляться на етапи, оплата прив'язується до «результату», а замовник максимально дистанціюється від виконавця. Практичні спостереження і публічні оцінки профільних органів України та партнерських безпекових структур європейських держав дають підстави описувати цей механізм як систему «диверсій за викликом» або «gig-economy саботажу», де інформаційна платформа використовується для прихованої мобілізації злочинної активності.

У межах цієї моделі первинний пошук кандидатів здійснюється через моніторинг спільнот, у яких потенційні виконавці є найбільш уразливими до маніпуляцій: маргінальні або радикалізовані канали, групи з пошуку роботи, чати мігрантів і осіб у складному соціально-економічному становищі, а також спільноти, пов'язані з незаконною діяльністю, де вже наявні навички анонімності та прихованого пересування. Як ілюстративний приклад у відкритому просторі часто згадують канал @grey_zone (пов'язуваний із середовищем Wagner), де можуть використовуватися боти для ініціювання контакту та подальшої «обробки» кандидата. Важливо, що вербування не зводиться до одноразового «заклику», а вибудовується як поетапний процес, у якому підвищується тяжкість завдань і водночас накопичується компрометуючий матеріал для утримання виконавця у залежності.

Процес «pipeline-вербування» зазвичай структурований так, щоб виконавець до останнього моменту не усвідомлював реального замовника або інституційної прив'язки завдання, а сама діяльність «нормалізувалася», як нібито дрібна, швидка й безкарна. Типова логіка може бути описана такою послідовністю:

| Етап | Дія вербувальника | Завдання для об'єкта | Оплата |
|---|---|---|---|
| I. Фільтрація | Масова розсилка в чатах | «Напиши нам, якщо хочеш заробити 200$ за ніч» | — |

| Етап | Дія вербувальника | Завдання для об'єкта | Оплата |
|---|---|---|---|
| II. Тестове завдання | Перевірка готовності порушити закон | Нанести графіті, розклеїти листівки, сфотографувати ТЦК | $20–50 |
| III. Втягування | Створення «компромату» | Фотофіксація військової техніки або підпал авто (як «іспит») | $100–300 |
| IV. Диверсія | Прямий наказ через анонімний бот | Підпал релейної шафи залізниці, закладання СВП | $500–1700 |

Паралельно застосовуються технології приховування слідів і ускладнення атрибуції: оплата в криптовалюті (зокрема USDT або Monero), використання «втемну» (false flag), коли вербувальник видає себе за представника українських органів або «партизанських» груп та пропонує завдання нібито «в інтересах України», а також видалення переписки через таймери самознищення і видалення чатів для обох сторін. Ознаками, що мають превентивне значення для розпізнавання вербувальника, зазвичай виступають підкреслена анонімність акаунта (відсутність реального фото, історії профілю, верифікованих даних), наполегливий стиль комунікації та швидка реакція після первинного контакту, вимога обов'язкового відеозвіту, як умови оплати, а також комунікація через посередницькі бот-інтерфейси замість прозорої ідентифікації контактної особи. Саме останній елемент – посередницькі боти – свідчить про перехід від ситуативного вербування до технологічно організованих моделей рекрутингу.

У цьому контексті варто окремо відзначити автоматизацію первинного відбору виконавців через бот-інтерфейси, що переводить вербування з "ручного" формату у масштабовану цифрову процедуру. Такі боти виконують роль проміжної ланки між куратором і потенційним виконавцем: вони стандартизують контакт, збирають структуровані дані та формують масив анкет для подальшої сегментації і постановки завдань. Типовий алгоритм включає етап "анкетування", який імітує легальне працевлаштування або вступ до закритої спільноти, та містить запити про місце перебування (місто/район), наявність технічних можливостей (авто, смартфон із камерою, автономні джерела живлення, інструменти), а також питання, спрямовані на оцінку готовності до протиправної поведінки. Окремий ризик становлять спроби так званої "верифікації", коли від особи вимагають фото документів або відео з обличчям під приводом "безпеки" – фактично це може створювати підстави для подальшого шантажу та утримання виконавця у залежності. Функціонально така бот-інфраструктура забезпечує масштабованість, приховування куратора та високу швидкість залучення; додатково застосовується сегментація ролей – від виконавців деструктивних дій (підпали, напади, пошкодження майна) до «спостерігачів» (збирання фото/відео, фіксація переміщень) та «агентів впливу» (поширення дезінформації у локальних чатах), що підтверджує багаторівневий характер загрози та пояснює, чому Telegram-мережі здатні одночасно продукувати як інформаційні, так і диверсійні ефекти.

Юридичне значення викладеного полягає в тому, що кримінально-правова оцінка дій виконавця не залежить від того, як саме йому було «продано» завдання: помилкове уявлення про замовника або уявна «легальність» дії не нейтралізують складу злочину, якщо об'єктивно вчинене діяння завдає шкоди обороноздатності, сприяє ворогу або посягає на громадську безпеку. Тому на рівні превенції необхідним є формування стандартів належної обачності для громадян і організацій, які взаємодіють у Telegram: розпізнавання «червоних прапорців» ботів-вербувальників, фіксація доказів комунікації, пріоритет повідомлення у визначені офіційні канали та відмова від будь-яких «завдань», що передбачають фото/відеозйомку чутливих об'єктів, збір геоданих, тестування мереж чи інші дії з очевидним розвідувальним або диверсійним потенціалом. У ширшому вимірі це повертає до вже окресленого нормативного

акценту на верифікації джерел і процедурній дисципліні: у Telegram безпекова помилка часто має не лише інформаційний, а й кримінально-правовий вимір, а отже режим користування платформою в секторі безпеки і оборони (та в суспільстві загалом) має розглядатися як елемент правової політики мінімізації шкоди.

Контрзаходи СБУ та підрозділів кіберполіції в цьому сегменті спрямовані на одночасне обмеження інфраструктури вербування і документування доказової бази для притягнення виконавців та організаторів до відповідальності. На організаційному рівні йдеться, зокрема, про системний моніторинг ризикових сегментів Telegram-середовища (радикальні спільноти, «робочі» чати, мережі із підозрілими оголошеннями), а також про взаємодію з платформою щодо реагування на виявлені боти й канали, які використовуються для вербування або координації протиправних дій. У межах превентивного контуру застосовуються також офіційні цифрові канали для прийому повідомлень про спроби вербування; показовим прикладом є запуск СБУ офіційного чат-бота «Спали» ФСБешника (@spaly_fsb_bot), який позиціонується як інструмент повідомлення про вербувальні контакти та підозрілу активність.

На процедурно-доказовому рівні ключове значення має те, що уявлення про «повну анонімність» у Telegram не відповідає реальним можливостям цифрової криміналістики та контррозвідувальної роботи. Навіть за умови видалення переписки або використання режимів самознищення повідомлень, ідентифікація виконавців може здійснюватися за сукупністю непрямих цифрових слідів: метаданих і телекомунікаційних параметрів (зокрема фіксації активності пристроїв у зоні події та часової кореляції), аналізу поведінкових патернів у мережі, а також матеріальних і візуальних маркерів у відеозвітах, які нерідко вимагають «куратори» як умову оплати. Додатковим каналом викриття стають фінансові сліди, оскільки практики розрахунків, попри декларовану оплату криптовалютою, на практиці часто комбінуються з переказами через посередників або з операціями, які можуть бути співвіднесені з уже відомими підозрілими гаманцями чи P2P-транзакціями. Загалом саме поєднання телекомунікаційних даних, цифрової криміналістики та фінансової аналітики формує той доказовий «ланцюг», який дозволяє переходити від загальної інформації про інцидент до конкретної особи та її комунікаційних зв’язків.

Порівняльний контекст підтверджує, що описані моделі «саботажу за наймом» є не локальним явищем, а частиною ширшої тактики РФ у Європі, де вербування через Telegram, оплата у криптовалюті та «дистанційне» керування низькорівневими виконавцями розглядаються як інструменти створення хаосу при збереженні заперечуваності. Це відображено в журналістських розслідуваннях про механіку рекрутингу через Telegram-боти (зокрема матеріалі OCCRP [9] про вербування для підпалів, саботажу та насильницьких дій), а також у медіа-описах європейських кейсів, де наголошується на «одноразовості» виконавців та їхній уразливості до викриття.

У підсумку, контрзаходи СБУ та кіберполіції у цій площині мають подвійний ефект: з одного боку, вони спрямовані на зменшення «пропускної здатності» вербувальної інфраструктури (боти/канали/мережі контактів), з іншого – забезпечують доказовість для кримінально-правової реакції, що, у свою чергу, підсилює превентивний сигнал для потенційних виконавців. Для правового виміру статті це важливо тим, що демонструє: державна політика реагування не зводиться до декларативних заборон використання платформи, а передбачає комбінацію організаційних, технічних і процесуальних інструментів – від верифікації каналів взаємодії до фіксації цифрових доказів і фінансового профілювання ризикових транзакцій.

У сукупності наведені контрзаходи демонструють, що державне реагування на ризики Telegram у секторі безпеки і оборони не може обмежуватися заборонами чи ситуативними попередженнями. Йдеться про формування інституційного режиму безпечного користування

платформою, який поєднує оперативне блокування та моніторинг вербувальних мереж, інструменти цифрової криміналістики, фінансову аналітику й процесуальну фіксацію доказів, а також організаційні канали для повідомлення про спроби вербування. Саме така комплексність підтверджує, що Telegram одночасно є ресурсом комунікаційної стійкості та середовищем підвищених ризиків, а отже потребує не лише технічних рішень, а й чіткої юридичної рамки з визначеними межами допустимої поведінки та механізмами відповідальності.

Підсумовуючи наведене, Telegram у сучасній війні виступає не просто каналом комунікації, а соціотехнічною інфраструктурою, в якій одночасно відбуваються мобілізаційні, інформаційні, розвідувальні й криміногенні процеси. Його використання у секторі безпеки і оборони може бути ефективним лише за умови поєднання інструментальної корисності (боти, моніторинг, OSINT, гуманітарні пошуки) з адміністративно-правовими обмеженнями, комплаєнс-процедурами та кримінально-правовими запобіжниками, що відмежовують допустимі практики від дій, які прямо або опосередковано сприяють противнику.

Висновки. Проведене дослідження засвідчує, що Telegram в умовах повномасштабної війни функціонує як соціотехнічна інфраструктура подвійного призначення: одночасно як канал оперативного пошуку та збору інформації для потреб безпеки і оборони (через офіційні боти, краудсорсинг повідомлень, моніторингові сповіщення, OSINT-опрацювання відкритих джерел, гуманітарний пошук і волонтерську логістику) і як середовище підвищених кібербезпекових та контррозвідувальних ризиків (витоки даних, підміна автентичних каналів, соціальна інженерія, масштабоване вербування «одноразових агентів» і організація диверсій за логікою «gig-economy саботажу»). У такій конфігурації ефективність використання платформи у секторі безпеки і оборони не може забезпечуватися виключно технічними засобами кіберзахисту або суто забороннними рішеннями, оскільки реальна практика комунікації й обігу інформації виходить за межі службових пристроїв і охоплює суспільні, волонтерські та змішані контури взаємодії. Відтак релевантною є комплексна модель правового реагування, яка поєднує інституціоналізовані адміністративно-правові обмеження службового використання із регламентованими дозволеними сценаріями, комплаєнс-процедурами, підготовкою персоналу, а також стандартами верифікації джерел і процедурної дисципліни в обігу цифрових відомостей.

У правовому вимірі принциповим є розмежування повідомлень превентивного характеру «про загрозу», що сприяють безпеці населення, і повідомлень про військові об’єкти, переміщення, наслідки уражень або інші чутливі дані, які можуть створювати розвідувальну цінність для противника та підпадати під кримінально-правові заборони. Зроблено висновок, що OSINT-практики у середовищі Telegram не є «поза правом»: їх допустимість визначається фактичним змістом дій, воєнно-правовим контекстом, чутливістю поширюваних відомостей і наявністю санкціонованих каналів взаємодії з уповноваженими органами, а не самим найменуванням методу. Окремо встановлено, що ворожа модель «диверсійного краудсорсингу» використовує технологічну масштабованість Telegram (канали, боти, анонімізацію, крипторозрахунки, false flag-легенди) для дистанціювання організаторів від виконавців і швидкого втягування у протиправну діяльність за поетапною «воронкою» завдань, що потребує нормативно і організаційно закріплених стандартів належної обачності, виявлення «червоних прапорців» вербування, пріоритету повідомлення у визначені офіційні канали та відмови від будь-яких «завдань», пов’язаних із фіксацією або передаванням чутливих даних.

Показано, що контрзаходи СБУ та підрозділів кіберполіції у цій сфері мають не лише превентивний, а й доказово-процесуальний ефект: поєднання моніторингу ризикових сегментів Telegram-середовища, взаємодії з платформою щодо реагування на боти/канали, застосування офіційних каналів прийому повідомлень, цифрової криміналістики, телекомунікаційних даних і фінансової аналітики формує доказовий «ланцюг», який руйнує уявлення про повну анонімність і забезпечує притягнення до відповідальності. Отже, оптимальна траєкторія державної політики полягає у формуванні режиму контрольованого та регламентованого використання Telegram у секторі безпеки і оборони, який зберігає інструментальну корисність платформи для

комунікаційної стійкості й краудсорсингу, але мінімізує її руйнівний потенціал у вимірах кібербезпеки, інформаційної безпеки та контррозвідки.

## ЛІТЕРАТУРА

1.Баловсяк Н. Комунікація державних органів України у телеграмі в умовах ризиків та обмежень. [Електронний ресурс]. — Режим доступу: https://intcom.kubg.edu.ua/index.php/journal/article/view/429 (дата звернення: 17.02.2026).
2.Анонімні та офіційні Telegram-канали в Україні: аналіз популярності під час гібридної війни. [Електронний ресурс]. — Режим доступу: https://cimc.knu.ua/uk/article/view/3826 (дата звернення: 17.02.2026).
3.Запорожець В. Небезпека використання Telegram та його вплив на українське суспільство. Кібербезпека: освіта, наука, техніка. 2024. [Електронний ресурс]. — Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/648 (дата звернення: 17.02.2026).
4.Івкова В. OSINT-технології як загроза кібербезпеці держави. Кібербезпека: освіта, наука, техніка. 2025. [Електронний ресурс]. — Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/749 (дата звернення: 17.02.2026).
5.Роль OSINT-досліджень у підвищенні рівня національної безпеки України: матеріали круглого столу (м. Львів, 7 травня 2025 р.). Львів: ЛьвДУВС, 2025. [Електронний ресурс]. — Режим доступу: https://dspace.lvduvs.edu.ua/bitstream/1234567890/8875/1/07_05_2025.pdf (дата звернення: 17.02.2026).
6.Gordiienko T. The use of digital platforms in a crisis: the case of Telegram and the impact of war on media consumption (case of Ukraine after 2022). 2025. [Electronic resource]. — Available at: https://ekmair.ukma.edu.ua/items/cef6c95a-a2ae-4a1a-be0b-a0e4fb004cc5 (accessed: 17.02.2026).
7.Використання Telegram: доступ до інформації vs загроза нацбезпеці: аналітичний матеріал. [Електронний ресурс]. — Режим доступу: https://niss.gov.ua/news/komentari-ekspertiv/vykorystannya-telegram-dostup-do-informatsiyi-vs-zahroza-natsbezpetsi (дата звернення: 17.02.2026).
8.Повідомлення РНБО/НКЦК про обмеження використання Telegram на службових пристроях (20.09.2024).
9.OCCRP. ‘Make a Molotov Cocktail’: How Europeans Are Recruited Through Telegram… (26.09.2024).
10.Офіційний сервіс «єВорог».
11.Bot STOP Russian War (@stop_russian_war_bot) та публічні повідомлення про його використання.
12.Додаткові матеріали про вербування/використання молоді у диверсіях (аналітика медіа).
13.Закон України «Про медіа» від 13.12.2022 № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

_

Дата першого надходження рукопису до видання: 21.02.2026
Дата прийнятого до друку рукопису після рецензування: 15.03.2026
Дата публікації: 17.04.2026