УДК / UDC: 351.746.1:004.738.5
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364488

Олександр Миколайович Поляков
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України
Київ, Україна
ORCID: https://orcid.org/0000-0002-8984-1476

ЗАГРОЗЛИВІ ТЕНДЕНЦІЇ ПОШИРЕННЯ ТЕРОРИСТИЧНОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ ТА ПРОПАГАНДИ ТЕРОРИЗМУ

Анотація. *Визначено загрози поширення терористичного контенту та пропаганди тероризму. Деталізовано напрями використання мережі Інтернет, соціальних мереж та онлайн платформ з терористичною метою. Окреселено шляхи використання терористами технологій штучного інтелекту з метою генерації пропаганди та радикалізації через месенджери та відеоплатформи. Розкрито механізми здійснення терористичної активності у мережі Інтернет, соціальних мережах та онлайн платформах. Узагальнено способи використання онлайн-трансляцій у реальному часі (стримінгу). Підсумовано, що поширення терористичної пропаганди включає загальнодоступні анонімні проксі-сервери, сервіси анонімізації, такі як "Tor" (Даркнет), віртуальні фінансові операції з використанням криптовалют. Визначено особливості краудфандингу як інструменту фінансування пропаганди тероризму, використання спеціальних сервісів, таких як тумблери та міксери. Розкрито напрями діяльності міжнародної спільноти, спрямовані на запобігання використання Інтернету і соціальних мереж для пропаганди тероризму, радикалізації суспільства. Зроблено висновок, що поширення терористичного контенту та пропаганди тероризму перетворилося на високотехнологічну, децентралізовану та гібридну загрозу у світових масштабах, а у фокусі такої злочинної діяльності перебуває переважно молодь, яка є уразливою та сприймає тероризм як розвагу. Підсумовано, що для поширення терористичного контенту активно використовуються: краудфандингові сервіси, месенджери та соціальні мережі. Визначено, що сучасні методи боротьби з терористичним контентом еволюціонували від ручного видалення постів до використання автономних систем на базі технологій штучного інтелекту. Узагальнено подальші шляхи удосконалення вітчизняного законодавства щодо посилення заходів у сфері боротьби з поширенням терористичного контенту в мережі Інтернет та пропаганди тероризму.*

Ключові слова: *терористичний контент, пропаганда тероризму, соціальні мережі, радикалізація, тероризм, месенджери, загрозливі тенденції, технології штучного інтелекту, технології анонімізації, краудфандингові сервіси, фінансування тероризму, медіа-сервіс.*

© Поляков О.М. 2026

Oleksandr M. Poliakov
Ukrainian Scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine
Kyiv Ukraine
ORCID: https://orcid.org/0000-0002-8984-1476

DANGEROUS TRENDS IN THE SPREAD OF TERRORIST CONTENT ON THE INTERNET AND TERRORIST PROPAGANDA

Summary. *The threats of the spread of terrorist content and terrorist propaganda are identified. The directions of using the Internet, social networks and online platforms for terrorist purposes are detailed. The ways in which terrorists use artificial intelligence technologies to generate propaganda and radicalization through messengers and video platforms are outlined. The mechanisms of terrorist activity on the Internet, social networks and online platforms are revealed. The methods of using online broadcasts in real time (streaming) are summarized. It is concluded that the spread of terrorist propaganda includes publicly available anonymous proxy servers, anonymization services such as "Tor" (Darknet), virtual financial transactions using cryptocurrencies. The features of crowdfunding as a tool for financing terrorist propaganda, the use of special services such as tumblers and mixers are identified. The directions of the international community's activities aimed at preventing the use of the Internet and social networks for terrorist propaganda and radicalization of society are disclosed. It is summarized that the spread of terrorist content and terrorist propaganda has turned into a high-tech, decentralized and hybrid threat on a global scale, and the focus of such criminal activity is mainly young people who are vulnerable and perceive terrorism as entertainment. It is summarized that crowdfunding services, messengers and social networks are actively used to spread terrorist content. It is determined that modern methods of combating terrorist content have evolved from manual removal of posts to the use of autonomous systems based on artificial intelligence technologies. Further directions of improving domestic legislation to strengthen measures in the field of combating the spread of terrorist content on the Internet and terrorist propaganda are summarized.*

Keywords*: terrorist content, terrorist propaganda, social networks, radicalization, terrorism, messengers, threatening trends, artificial intelligence technologies, anonymization technologies, crowdfunding services, terrorist financing, media service.*

Постановка проблеми. Сучасна модель глобалізації сприяє розширенню географії тероризму, зокрема у кіберпросторі. З появою мережі Інтернет терористи використовують його як свій майданчик для швидшого поширення своєї ідеології з метою охоплення дедалі більшої кількості людей. Одним із важливих небезпечних напрямків тероризму залишається поширення терористичного контенту в мережі Інтернет та пропаганда терористичної діяльності. Анонімність та легкість цифрових комунікацій роблять Інтернет ідеальним злочинним інструментом для міжнародних терористичних груп щодо поширення ними своєї ідеології, вербування нових членів та планування майбутніх атак. Нерегульоване онлайн-середовище сприяє радикалізації та поширенню ідеології тероризму, що призводить до виникнення реальної проблеми у світової спільноти в контексті боротьбі з тероризмом, особливо коли терористичний контент стає вільно поширюваним у відкритому доступі без будь-яких обмежень. Тенденційна загроза поширення терористичного контенту в мережі Інтернет є однією з найсерйозніших та небезпечних в сучасних умовах. Адже терористичні організації намагаються активно використовувати онлайн-платформи для поширення радикалізації,

рекрутингу, пропаганди тероризму з метою залякування і подальшої координації своїх злочинних дій.

Сприятливі можливості терористичних організацій та їхній доступ до технічних ресурсів, платформ, соціальних мереж в режимі реального часу роблять мережу Інтернет одним із найважливіших інструментів в їхньому арсеналі, який використовується задля інтерактивного навчання, обміну технічними знаннями онлайн та створення децентралізованих пропагандистських структур, що значно ускладнює для правоохоронних органів здійснення постійного моніторингу та запобігання терористичній діяльності. Саме поширення пропаганди ідеології тероризму з використанням мережі Інтернет є досить простим процесом, який не вимагає наявності спеціальних знань, вмінь та навичок, а технічні витрати на передавання певного повідомлення, зберігаючи при цьому анонімність його відправника, є досить низькими, при цьому відповідне повідомлення може поширюватися й тиражуватися без попередньої цензури чисельну кількість на абсолютній високій швидкості. Це дозволяє широкому загалу користувачів дізнаватися про повідомлення, які поширює терористична організація, навіть тим, хто не є прямими одержувачами такого виду кореспонденції. Завдяки цьому терористична організація отримує шалений розголос або набуває скандальної популярності та, зрештою формує штат нових прихильників, анонсує майбутні здійснення тієї чи іншої атаки або бере на себе відповідальність за вчинення теракту.

У свою чергу, штучний інтелект має потужний потенціал для збільшення обсягів зловмисного використання сучасних передових технологій у терористичних цілях. Сучасні тенденції поширення терористичного контенту демонструють перехід до високотехнологічних та децентралізованих методів, що ускладнює його моніторинг та застосування своєчасних заходів протидії. В сучасну епоху основною загрозою залишається використання штучного інтелекту для генерації пропаганди та радикалізація через месенджери та відеоплатформи. Від дипфейкових відео, розроблених для маніпулювання громадською думкою, до швидко генерованої пропаганди, що підживлює радикалізацію, терористи знаходять нові способи використання цих інструментів для досягнення своїх злочинних цілей. Одночасно поряд із динамічним розвитком технологій штучного інтелекту зростають і ризики, які він становить для глобальної безпеки. За таких умов автоматизоване поширення ідеології пропаганди тероризму та терористичного контенту в мережі Інтернет вбачається новим викликом і одночасно загрозою для усього цивілізованого світу. Враховуючи викладене, доцільним є визначення та узагальнення загрозливих тенденцій у сфері використання технологій штучного інтелекту для поширення терористичного контенту в мережі Інтернет та пропаганди терористичної діяльності, що набуває особливої актуальності в умовах правового режиму воєнного стану в контексті тривалої російської військової агресії проти України.

Результати аналізу наукових публікацій. Проблематику забезпечення захисту кіберпростору від терористичних організацій, використання новітніх технологій для попередження терористичних загроз, пошук оптимальної моделі та сучасних механізмів для запобігання поширенню терористичної ідеології через медіа та мережу Інтернет здійснювали у своїх наукових працях: Л. Войніч [1], О. Довгань, І.Доронін [2], І. Озерчук [3], А. Мовчан та М. Мовчан [4], І. Ткачов і С. Ільченко [5], О.Поляков [6] та ін. Протидія тероризму як напрям гарантування системи національної безпеки в інформаційній сфері перебував у фокусі уваги таких науковців як: Т. Лиськи, О. Клімук та Д. Лисянської [7], Б Леонова та С. Лихової [8], А. Помаза-Пономоренко [9],

Д. Харамурзи [10] та інших науковців. Проте жоден із вказаних науковців предметно не розглядав загрозливі тенденції поширення терористичного контенту в мережі Інтернет та здійснення пропаганди тероризму, що посилює актуальність цієї публікації.

Метою статті є визначення та деталізація на підставі проведеного аналізу загроз поширення терористичного контенту, здійснення пропаганди тероризму в мережі Інтернет в контексті уточнення пріоритетів та подальших шляхів удосконалення законодавчої бази у сфері боротьби з терористичною діяльністю у мережі Інтернет.

Виклад основного матеріалу. Останнім часом спостерігається підвищена терористична активність у мережі Інтернет. Зокрема, цифрові технології надали безпрецедентні можливості для терористів щодо побудови їхньої комунікації та здійснення інформаційно-просвітницької роботи задля поширення ідеології та пропагади тероризму, які використовують інноваційні методи та платформи з метою швидкої передачі повідомлень між своїми членами та прихільниками. Окрім своїх закритих веб-сайтів, електронних журналів та публікацій, терористичні угрупування широко використовують такі зашифровані безпечні соціальні мережі, як “Telegram”, “Facebook”, “Signal”, інші ресурси та форуми з метою координації своєї протиправної діяльності, організації вербування нових членів і одночасного поширення пропаганди ідеології тероризму, що дозволяє їм уникнути виявлення з боку правоохоронних органів. Використання даркнету для поширення пропаганди та оперативної координації підкреслює привабливість цієї платформи для терористичних груп. Окрім створення своїх онлайн-платформ, терористи використовують інтерактивні інструменти, такі як чати, блогосфера, сайти обміну відео та платформи, такі як “MySpace”, “Twitter”, “Instagram” та “YouTube” для навчання та інструктажу.

Штучний інтелект може використовуватися у злочинних цілях для посилення інтенсивності терористичних атак або для посилення потенціалу терористичних груп або окремих осіб поширювати екстремістську пропаганду та підбурювати до насильства [11]. На цьому фоні терористи активно використовують технології штучного інтелекту, які докорінно змінюють ландшафт цифрового тероризму, роблячи пропаганду більш масовою, персоналізованою та важкою для виявлення та блокування. Сучасні тенденції у цій площині переконливо демонструють загрози та виклики, які першочергово пов’язані із використанням з боку терористів новітніх технологій для здійснення генерації пропаганди з використанням багатомовного контенту у соціальних мережах, а також на таких платформах як “TikTok” та “Discord”, у зашифрованих месенджерах і навіть за допомогою ігрових та розважальних платформ. За допомогою цих технологій клонують голоси, автоматично перекладають і синтезують мовлення для адаптації своїх ідеологічних матеріалів різними мовами світу. При цьому терористичний контент швидко поширюється завдяки вірусним механізмам і доволі часто переміщується на менш модеровані платформи навіть після повного видалення.

Техології штучного інтелекту дозволяють терористичним організаціям за лічені секунди адаптувати радикальні матеріали десятками мов, зберігаючи стилістику та емоційне забарвлення. Так, наприклад, на платформі “Rocket.Chat”, яку активно використовує “ІДІЛ”, у жовтні 2025 року з’явилося відео з японськими субтитрами, створеними за допомогою технологій штучного інтелекту [12]. Тобто використання інструментів автоматичного перекладу робить терористичні заклики доступними та зрозумілими для ширшої аудиторії в різних державах світу. Адже не лише “ІДІЛ”, але й інші теористичні організації і радикально екстремістськи налаштовані угрупування активно користуються безоплатними інструментами штучного інтелекту, зокрема “ChatGPT”, “Gemini” та “GROK”, застосовуючи ці технології як для створення

візуального контенту, так і для оптимізації планування та розвідки своєї перспективної терористичної діяльності. Маніпулятивні повідомлення, згенеровані за допомогою штучного інтелекту, вдосконалюються настільки, що їх дедалі важче відрізнити від справжніх, чим і намагаються скористатися терористи.

Штучний інтелект застосовується для створення терористами фейкових новинних сайтів, що імітують офіційні медіа для маніпулювання громадською думкою. За допомогою штучного інтелекту відбувається візуальна маніпуляція, створення терористами реалістичних відео або аудіо із закликами від імені відомих політиків, релігійних лідерів або лідерів думок для дестабілізації суспільства. Важливою складовою арсеналу терористів також є фабрикація подій: генерація фото- та відеодоказів "злочинів" або "нападів", яких не було насправді, щоб спровокувати агресію або помсту; автоматизація текстів, що передбачає використання ними великих мовних моделей для написання маніпулятивних статей, постів та маніфестів, що виглядають як професійна журналістика. Алгоритми штучного інтелекту можуть аналізувати профілі користувачів у соцмережах, виявляючи їхні образи, побоювання чи психологічний стан, щоб спрямовувати на них максимально точний і "болючий" контент. Терористи також активно застосовують AI-чатботи, що призводить до створення віртуальних "наставників" або "рекрутерів", які ведуть діалоги з потенційними жертвами у форматі 24/7, поступово схиляючи їх до вчинення терористичних актів.

Останнім часом терористи використовують практику створення нейроблогерів та ботів з ШІ-генерованими обличчями та біографіями, які імітують активність реальних людей, ілюзію масової підтримки радикальних ідей та сприяють поширенню ідеології пропаганди тероризму. Якщо раніше для створення якісної пропаганди потрібні були цілі медіацентри, то тепер достатньо лише одного оператора і наявного відповідного програмного забезпечення. Адже алгоритм також можна легко обійти, модифікувавши зображення чи відео, щоб вони не розпізнавалися системою. Втім, штучний інтелект не є таким ідеальним, як здається, оскільки він припускається численних помилок: не відрізняє аналітичний матеріал від закликів до тероризму, видаляючи легальну інформацію. Штучний інтелект може автоматично змінювати код відео, піксельну структуру зображень або формулювання тексту так, щоб вони залишалися зрозумілими для людини, але були "невидимими" для стандартних фільтрів безпеки соцмереж, які активно використовують автоматичні алгоритми для пошуку терористичного контенту.

Так, наприклад у березні 2026 року Meta оголосила про запровадження нових систем захисту контенту на основі технологій штучного інтелекту. Завдання, пов'язані із контролем за контентом, включатимуть виявлення та видалення протиправного контенту, зокрема який присвячений тероризму, наркотикам [13]. Окрім того, у світі триває активне розроблення універсальних інструментів для автоматичного розпізнавання фейкового контенту, у тому числі й терористичного спрямування, на основі штучного інтелекту, при цьому ці сервіси відрізняються рівнем доступності, точністю, технічними характеристиками й орієнтацією на різні медіаформати [14, с.5]. Жодна платформа не може гарантувати абсолютної захищеності від терористичного контенту, адже основне питання полягає виключно у прагненнях мінімізації шкоди та пошуку можливостей задля блокування протиправного контенту.

Пропаганда ідеології тероризму включає публічні заклики до вчинення терористичних актів, тлумачення та обгрунтування причин та передумов тероризму, може існувати як у формі прямого підбурювання до насильства, так і непрямого, що включає глорізацію та виправдання вчинення терористичних актів, що створює

одночасно небезпеку імітації. Інформаційне функціональне крило терористичних організацій перебуває в активному пошуку охочих долучитися до протиправної діяльності. Одночасно із розвитком функціонального наповнення соціальних мереж зросла й кількість способів "схилити" нових учасників до терористичної діяльності. При цьому онлайн-діяльність терористів переважно спрямована на іноземну аудиторію з метою вербування нових членів, проведення рекрутингу у соціальних мережах. Рекрутингові компанії зазвичай включають: тривале приватне листування у "Facebook", "Twitter" і "WhatsApp", надання підписки на закриті канали та платформи та спрямовують свої зусилля переважно на молодь з використанням функції багатомовності. Також активно використовується функція рекламного таргетингу, завдяки чому пропаганду можна поширювати на конкретні аудиторії, адаптуючи заклики приєднатися до терористичної діяльності у відповідності до схильності соціальних груп.

Наприклад, шалено популярний серед молоді «Snapchat», який лідирує на цифрових ринках Південної Азії, Північної Америки та Західної Європи, де 850 млн. користувачів часто використовується терористами для рекрутингу молоді за допомогою коротких відео та влучних фраз, які привертають увагу до публікації. Цією платформою користується 430 млн. щодня, а основна аудиторія – молодь від 13 до 35 років. Також терористи можуть створювати фейкові акаунти публічних діячів, відомих світових акторів, співаків і активістів, що мають значний вплив на молодь, або використовують їх оригінальні акаунти для розкрутки власного протиправного контенту, що можливо завдяки надання першим коментаря допису особи з багатьма підписниками: коментар буде помітний усім наступним читачам, таким чином поширюючи інформацію на різні аудиторії.

На відміну від залякувань та вимог, пропаганда тероризму виглядає набагато "привабливішою" для користувачів. Своєю чергою, відео, які викладаються в "Youtube", спрямовані на пропаганду, містять лише визнання відповідальності за певні терористичні акти, проте часто не зображують акти насилля. Крім закликів долучитися до активностей діяльності своєї організації, терористи поширюють так званий "освітній" контент для радикалізованої молоді: як можна виготовити вибухівку в домашніх умовах, поводитися зі зброєю, обрати місце та час для вчинення терористичного акту тощо. Не менш популярним серед терористів є поширення фейків та іншої неправдивої інформації щодо методів протидії національних урядів радикальним організаціям з метою викликати в аудиторії користувачів співчуття і прихильність до власної позиції. Також терористи часто апелюють до загальних вразливих понять, таких як: "дискримінація", "політичні переслідування", щоб виправдати свою неспроможність діяти законними методами. Деякі терористичні організації не зупиняються на публікації відео і здійснюють оприлюднення онлайн-публікацій, які містять інтерв'ю з учасниками цих організацій, розповіді про позитивні сторони та мету своєї діяльності, інформування про можливість поповнення кадрового потенціалу, умови й порядок долучення до лав того чи іншого терористичного угруповання тощо. Завдяки існуванню сотен тисяч фейкових акаунтів інформація поширюється на величезні аудиторії користувачів соціальних мереж. Не менш оригінальним способом є публікація нейтрального допису на соціально важливу тему і подальше редагування його змісту, коли публікація отримує велику кількість уподобань та лайків, стає популярною на тій чи іншій платформі. Іншим способом є надання посилань на сайти терористів у дописах з нейтральним контентом. Наразі механізму відслідковування таких публікацій, на жаль,

не існує, втім, кількість осіб, які піддаються впливу подібних матеріалів, є надзвичайно великою.

Також існують спеціальні ресурси для терористичної пропаганди і налагодження внутрішньої комунікації, як-от власні веб-сайти, месенджери, закриті форуми, які активно використовується терористами. Так, наприклад 23 березня 2026 року представники Аль-Каїди оприлюднили текст посібника, в якому містяться інструкції щодо виготовлення вибухового пристрою з використанням комерційно доступних матеріалів [15]. Актуальною проблемою залишається й те, що соціальні мережі здебільшого зосереджують увагу на протидії міжнародному тероризму (першочергова реакція на дописи ІДІЛу, Хезболли, Аль-Каїди), при цьому забуваючи про національні контексти. Особливо брак регулювання простежується у державах, де платформи не мають локальних модераторів контенту. Розпочата 28 лютого 2026 року ескалація конфлікту та суттєве погіршення безпекової ситуації на Близькому Сході призвели до появи проіранського терористичного угрупування "Ашаб аль-Ямін", яка активно використовує пов'язані з Іраном Telegram-канали, що використовуються для поширення пропаганди іранського уряду, вербування своїх прихільників по усій Європі [16]. Для підвищення чутливості та одночасно зацікавленості населення до терористичної діяльності, організації оприлюднюють на власних ресурсах, які переважно використовує молодь, як-от "TikTok", "Snapchat" чи "Instagram" "шокуючий" контент, де прямо демонструються результати чи процес здійснення терористичних атак, жертви тощо. Оголошення про майбутні терористичні атаки супроводжуються шокуючими відео трансляціями та зображеннями, що пояснюється прагненням терористів будь-якою ціною привернути увагу спільноти до своєї злочинної діяльності. Зокрема, особливо гучні активності в соцмережах найчастіше потрапляють до медіа – що лише сприяє терористам, допомагаючи поширювати їм свої вимоги до урядів держав і міжнародних організацій.

Використання онлайн-трансляцій у реальному часі (стримінгу) стало однією з найнебезпечніших стратегій сучасного тероризму, що надає змогу зловмисникам створювати "ефект присутності", миттєво поширювати паніку та радикалізувати глядачів в обхід традиційних засобів модерації. Стримінгові платформи, орієнтовані на геймерів, використовуються для відтворення сценаріїв терористичних актів у 3D-іграх з подальшою трансляцією. Такий формат особливо привабливий для залучення та вербування молоді. Під час трансляцій у реальному часі терористи використовують чати для прямої комунікації з глядачами, відповідаючи на питання та поступово залучаючи вразливих осіб до закритих груп. Навіть якщо трансляція триває лише кілька хвилин і її бачить невелика кількість людей, контент миттєво записується та перезаливається на тисячі дзеркальних сайтів і менш модерабельних платформ (наприклад, Telegram). Терористи використовують "YouTube", "Facebook Live" та "Twitch" для здійснення онлайн - трансляцій нападів у режимі реального часу. Це робиться для максимізації психологічного шоку та глорізації терористів у середовищі радикальних спільнот та дозволяє збирати великі аудиторії в режимі "прямого ефіру" з метою монетизації терористичного контенту або сприяння організації збору пожертв задля фінансової підтримки. Адже особливу небезпеку становлять саме онлайн-трансляції з метою реалізації тактики "атмосфери страху", що передбачає використаня мас-медіа для трансляції актів терору з метою психологічного тиску на населення та створення паніки. Для обходу автоматичних алгоритмів "YouTube" або "Facebook", терористи можуть накладати фільтри на відео, змінювати кодування або додавати музичний супровід, що ускладнює розпізнавання ШІ-системами.

Важливою складовою злочинної діяльності терористів є пошук нових каналів отримання фінансування. Використання технологій анонімізації та криптоактивів створює “цифрову фортецю”, яка дозволяє терористичним організаціям функціонувати автономно від державних фінансових та наглядових систем. Поширення терористичної пропаганди включає загальнодоступні анонімні проксі-сервери, сервіси анонімізації, такі як “Tor” (Даркнет), віртуальні фінансові операції з використанням криптовалют, що надає змогу хостити сайти з пропагандою та форуми для вербування на спеціальних доменах, які не індексуються звичайними пошуковими системами. Проксі-сервери та VPN допомагають терористам обходити національні фаєрволи, отримувати доступ до заблокованих соцмереж з метою поширення терористичного контенту. Останнім часом спостерігається перехід до мереж типу “P2P”, які ще важче відстежити, аніж “Tor”, через вищий рівень шифрування всередині спільноти. На цьому фоні криптовалюти стали основним інструментом фінансування тероризму. Досить зручними для отримання фінансування з боку терористів залишаються месенджери завдяки анонімності та низькому рівню модерації, де активно діють закриті радикальні спільноти. Вони дозволяють терористам безпосередньо контактувати з аудиторією та, водночас, залишатися непомітними для правоохоронних органів, використовуючи закриті спільноти, анонімні акаунти краудфандингових сервісів тощо. Так, зокрема краудфандинг став одним із найбільш важливих та дієвих інструментів фінансування тероризму, оскільки він маскує збір коштів під виглядом доброчинності.

Останнім часом ця тенденція набула нових специфічних рис, зокрема найпоширеніша тактика терористів у цьому сегменті — проведення кампаній для “допомоги біженцям”, “викупу полонених”, “будівництва шкіл та інших об’єктів соціальної інфраструктури” або “організації надання медичної допомоги постраждалим від конфліктів”. Емоційний контент досить часто посилюється завдяки ШІ-генерації фото та відео і спонукає звичайних користувачів до пожертв. Краудфандинг не лише забезпечує фінанси, а й працює як інструмент психологічного тиску, оскільки людина, яка зробила навіть невеликий фінансовий внесок або донат, відчуває причетність до “спільної справи”, що є першим кроком до повної радикалізації. При цьому, краудфандинг дозволяє залишатися інкогніто для органів правопорядку, тому активно використовується терористами по всьому світу. Подібні ситуації викликають занепокоєння національних правоохоронних органів. Зокрема, уряд Індонезії занепокоєний можливістю терористів використовувати фінансові ресурси, зібрані через краудфандингові сервіси з метою організації допомоги жертвам та їхнім родичам внаслідок вчинення терористичних актів. У Великобританії навіть були розроблені керівні принципи щодо захисту пожертв від зловживань з екстремістською або терористичною метою.

Так, наприклад, у 2025 році Канада, Великобританія, а у 2026 року і США оприлюднили свої дослідження, які присвячені національній оцінці ризиків відмивання грошей та фінансування тероризму [17; 18; 19], яке являє собою узагальнення загроз, ризиків та викликів, пов’язаних із фінансуванням тероризму в контексті поширення сучасних цифрових технологій, геополітичної напруженості та зростаючої складності виявлення терористичних мереж. Особлива увага у цих дослідженнях приділяється пошуку донорів тероризму в соцмережах, завдяки яким терористи отримують не лише фінансову, а й матеріальну підтримку (зброя, наркотичні речовини, підроблені документи тощо). Стратегії пошуку донорів терористичними організаціями еволюціонували від прямої підтримки з боку окремих держав (Ліван, Йемен) до створення складних децентралізованих фінансових мереж. Терористичні організації

активно використовують благодійні організації шляхом створення фіктивних фондів з метою перенаправлення частини зібраних коштів на потреби своїх терористичних осередків. Новий тренд — отримання пасивного доходу терористичними організаціями через стейкінг криптовалют, придбаних на кошти донорів, або відмивання грошей через внутрішньоігрові покупки в популярних онлайн-казіно. Виявлення донорів фінансування терористичних організацій досить складно, оскільки пожертви часто маскуються під легальну комерційну діяльність або оплату ІТ-послуг, одночасно використовується схема розпилення платежів, коли великі суми розбиваються на сотні дрібних трансакцій, які не привертають особливої уваги систем фінансового моніторингу та контролю.

Ще одним типовим способом є використання спеціальних сервісів, таких як тумблери та міксери, які змішують кошти від тисяч користувачів, що робить неможливим відстежити зв'язок між конкретним донорами і терористами. Існує чимало міксерів, які використовуються для здійснення анонімних переказів криптовалют. Проте більша частина з них є централізованими сервісами, які можуть зловживати довірою користувачів, викрадати їхні заощадження або особисті дані. Засновники криптовалютних міксерів неодноразово анонсували, що вони відіграють важливу роль з метою захисту користувачів та інвесторів. Терористами також активно використовуються Крос-чейн мости (cross-chain bridges) — сервіси, що дозволяють миттєво обміняти одну криптовалюту (наприклад, Ethereum) на іншу (наприклад, Monero) і перевести її в інший блокчейн, що розриває слід транзакції. Технологія "Zero-Knowledge Proofs" (ZKP) передбачає, що сучасні міксери використовуються як докази з нульовим розголошенням, який являє математичний метод, який дозволяє підтвердити транзакцію, не розкриваючи жодних даних про її учасників.

Враховуючи масштабування поширення терористичних загроз у сучасному світі, міжнародна спільнота прагне максимально запобігти використанню Інтернету і соціальних мереж з метою вчинення актів кібертероризму, радикалізації суспільства. З цією метою проводиться системна робота, яка спрямована на удосконалення національного та міжнародного законодавства, передбачається створення організаційно-правових засад задля розробки механізмів швидкого й оперативного видалення терористичного контенту у мережі Інтернет. При цьому, під час розробки ефективних засобів правового захисту в контексті заборони поширення терористичного контенту вимагається обов'язкове дотримання основних прав людини і громадянина, гарантованих як на національному, так і міжнародному рівнях. В контексті викладеного, світова спільнота переймається проблематикою поширення терористичного контенту в мережі Інтернет та пропаганди тероризму. Останнім часом міжнародна спільнота в особі регуляторів перейшла від точкових санкцій до системного наступу на криптовалютні міксери, розглядаючи їх як "першочергову загрозу відмивання грошей за участю терористів".

Основна стратегія полягає у позбавленні цих сервісів зв'язку з реальною економікою через жорсткий контроль фінансових посередників. У 2024 році в ЄС було створено новий контролюючий орган — Управління з питань боротьби з відмиванням грошей та фінансуванням тероризму (AMLA) [20], яке у рамках компетенції опікується питаннями протидії відмиванню коштів, здобутих злочинним шляхом, та здійснює координацію діяльності національних органів фінансової розвідки для забезпечення правильного та послідовного застосування правил щодо нагляду за криптосектором. Також відбувається посилення нагляду за стейблкоїнами: національні регулятори на постійній основі аналізують взаємодію міксерів зі стейблкоїнами та крос-чейн мостами з

метою виявлення та блокування шляхів подальшого виведення коштів, які спрямовуються на фінансування тероризму.

З метою обмеження доступу дітей та підлітків до онлайн платформ, Австралія стала першою державою у світі, яка запровадила заборону соціальних мереж для осіб віком до 16 років, при цьому відповідальність за дотримання заборони покладається не на користувачів чи батьків, а на платформи, яким загрожують десятки мільйонів доларів штрафів, якщо вони не дотримаються встановлених вимог [21].

Висновки. На підставі проведеного аналізу можна зробити висновок, що поширення терористичного контенту та пропаганди тероризму перетворилося на високотехнологічну, децентралізовану та гібридну загрозу у світових масштабах. Найбільше сприяння та важлива роль у цьому контексті відводиться терористами технологіям штучного інтелекту щодо створення діпфейків та автоматизованого перекладу пропаганди, що надає змогу радикалізувати аудиторію, долаючи мовні бар'єри. Використання мережі "Tor", месенджерів із низькою модерацією (Telegram) та сервісів змішування криптовалют (міксерів) створило автономну екосистему, що дозволяє терористам фінансувати свою діяльність та координувати атаки, залишаючись майже непомітними для традиційних банківських та правоохоронних систем. Пропаганда тероризму адаптується під молодь через онлайн-ігри та стримінгові платформи. Прямі трансляції терористичних актів створюють ефект співучасті, що максимізує психологічний тиск на суспільство та сприяє глоризації терористів в режимі реального часу. За таких умов можна підсумувати, що для поширення терористичного контенту використовують три типи платформ: краудфандингові сервіси, месенджери та соціальні мережі. Зокрема, краудфандинг став інструментом не лише збору грошей, а й вербування найманців з боку пересічених терористів. Маскуючись під благодійність, терористичні організації залучають тисячі "дрібних донорів", що робить фінансові потоки важкодоступними для здійснення будь-якої ідентифікації. Зручними для цілей отримання фінансування також є месенджери та соціальні мережі, які дозволяють терористам безпосередньо контактувати з аудиторією та, водночас, залишатися непомітними для правоохоронців.

Враховуючи загрозливі тенденції поширення терористичного контенту та пропаганди тероризму, існує потреба запровадження системного підходу, який має поєднати оперативність та ефективність видалення терористичного контенту, захист цифрових прав людини, розвиток медіаграмотності населення. Сучасні методи боротьби з терористичним контентом еволюціонували від ручного видалення постів до використання автономних систем на базі технологій штучного інтелекту. Адже видалення терористичного контенту є досить складним процесом, що поєднує юридичні, технічні та етичні виклики. Основна тенденція у цьому контексті — це перехід від "реагування на інциденти" до моделі прогнозування терористичних загроз, що включає самостійне виявлення платформами намірів та прагнень користувача щодо радикалізації ще на ранніх стадіях шляхом моніторингу його вподобань та аналізу мережевих зв'язків. Так, наприклад, месенджери (WhatsApp, Signal) впроваджують механізми сканування на пристрої користувача (on-device matching), що дозволяє знаходити та виявляти терористичні матеріали, не порушуючи при цьому наскрізне шифрування, яке запроваджено для здійснення приватного листування.

Основна проблематика полягає у необхідності швидкої реакції на вказані терористичні загрози при одночасному дотриманні прав людини та подоланні опору глобальних платформ, оскільки, соціальні мережі та месенджери, особливо "Telegram" досить часто ігнорують урядові запити на видалення протиправного контенту, який має

ознаки терористичного, посилаючись на внутрішню політику конфіденційності. Одночасно існує досить тонка межа між терористичною пропагандою та свободою слова чи журналістським висвітленням подій, у зв'язку з цим некоректна модерація може призвести до появи жорсткої цензури.

Своєю чергою, Україна розглядає обмеження доступу підлітків до онлайн-платформ за прикладом Австралії. Адже в Україні терористичний контент досить часто переплітається з російською пропагандою та дезінформацією, що вимагає від вітчизняних правоохоронних органів оперативного реагування, яке включає не тільки видалення відео чи текстів, а й проведення комплексного аналізу спеціальних інформаційних операцій, які проводить держава-агресор проти України. В контексті викладеного, Україна впевнено здійснює реалізацію курсу євроінтеграції, що передбачає імплементацію законодавства ЄС, зокрема Регламенту 2021/784 [22] (щодо боротьби з поширенням терористичного контенту в мережі Інтернет з метою запровадження системи моніторингу виявлення та видалення протиправного контенту постачальниками послуг хостингу), що вимагає приведення національного законодавства у відповідність до стандартів ЄС, створення чітких процедур для провайдерів, які надають відповідні послуги. Також вбачається доцільним прискорити прийняття Закону України "Про внесення змін до деяких законів України щодо регулювання діяльності платформ спільного доступу до інформації, через які поширюється масова інформація" (від 25.03.2024 року реєстр. № 11115), який спрямований на посилення захисту національних інтересів та прав користувачів медіа-сервісів.

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література

1. Wojnicz. L. New European Union Rules to Combat Terrorist Propaganda online. *Reality of Politics.* 2024. № 30. P. 102-116. DOI: 10.15804/rop2024408. URL: https://www.researchgate.net/publication/396007198_New_European_Union_Rules_to_Combat_Terrorist_Propaganda_Online.

2. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кібербезпеки: Монографія. Київ: Видавничий дім «АртЕк», 2017. 107 с.

3. Озерчук І.М. Проблеми забезпечення захисту кібепростору від діяльності терористичних організацій. *Інформація і право.* 2021. № 4 (39). С. 148-154.

4. Мовчан А.В., Мовчан М.А. Використання новітніх технологій для попередження терористичних загроз. *Соціально-правові студії.* 2020. Випуск 2 (8). С. 105-111.

5. Ткачов І.В., Ільченко Ю.О. Тероризм і медіа: огляд ролі медіа в поширенні терористичної пропаганди та міжнародного досвіду у протидії цьому явищу. *Юридичний науковий електронний журнал.* 2024. № 12. С. 274-277. URL: https://lsej.org.ua/12_2024/63.pdf.

6. Поляков О.М. Особливості протидії поширенню деструктивного контенту. *Інформація і право.* 2023. №1 (44). С. 129-141.

7. Лисько Т.Д., Клімук О.О., Лисянська Д.В. Інформаційний тероризм як загроза національній безпеці та спосіб інформаційної війни. *Юридичний науковий електронний журнал.* 2022. № 10. С. 574-576. URL: https://www.lsej.org.ua/10_2022/143.pdf.

8. Леонов Б. Д., Лихова С. Я. Інформаційний тероризм як загроза національній безпеці України. *Юридичний вісник.* 2021. №2. (59) С.170-176. URL: https://er.nau.edu.ua/bitstream/NAU/53546/1/22858.pdf.

9. Помаза-Пономаренко А.Л. Протидія тероризму як напрям гарантування системи національної безпеки: тренди та механізми. *Економіка, управління та адміністрування*. 2025. № 2 (112). С. 187-193.

10.Харамурза Д. Інформаційний тероризм як інструмент гібридної війни та фактор руйнації медіапростору. *Інтегровані комунікації.* 2023. № 2(16). С. 29-37. URL: https://www.intcom.kubg.edu.ua/index.php/journal/article/view/272/220.

11. Algorithms and terrorism: The Malicious use of artificial intelligence for terrorist purposes. United Nations Office of Counter-Terrorism (UNOCT), 2021. URL: https://unicri.org/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf.

12. Extremist Content Online: Rpo-ISIS RocketChat User Posts Alleged AI Conversation Regarding Explosives Use. URL: https://www.counterextremism.com/press/extremist-content-online-pro-isis-rocketchat-user-posts-alleged-ai-conversation-regarding.

13. Meta впроваджує нові системи захисту контенту на основі штучного інтелекту. URL: https://internetua.com/meta-vprovadjuye-novi-sistemi-zahistu-kontentu-na-osnovi-shtucsnogo-intelektu?utm_source=ukrnet_news.

14. Артеменкова О., Василенко В., Ковтун Л. Використання штучного інтелекту в соціальних мережах як зброї інформаційної війни. *Вісник Книжкової палати.* 2025. №8. С. 3-8.

15. Extremist Content Online: Al-Qaeda in the Arabian Peninsula Releases «Inspire Guide» Praising Bondi Beach Attack and Shares Bomb Making Instructions. URL: https://www.counterextremism.com/press/extremist-content-online-al-qaeda-arabian-peninsula-releases-inspire-guide-praising-bondi.

16. A shadowy, pro-Iranian group claimed a spate of attacks in Europe. But it might be a facade. URL: https://edition.cnn.com/2026/04/11/europe/iran-linked-hybrid-attacks-europe-intl.

17. 2025. Assessment of Money Laundering and Terrorist Financing Risks in Canada. URL: https://www.canada.ca/content/dam/fin/programs-programmes/fsp-psf/nira-neri/2025/nira-neri-2025-eng.pdf.

18.National Risk Assessment of Money Laundering and Terrorist Financing 2025. URL: https://assets.publishing.service.gov.uk/media/6877be59760bf6cedaf5bd4f/National_Risk_Assessment_of_Money_Laundering_and_Terrorist_Financing_2025_FINAL.pdf.

19. 2026 National Money Laundering Risk Assessment. URL: https://home.treasury.gov/system/files/246/2026-NMLRA.pdf.

20. The Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). URL: https://www.amla.europa.eu/index_en.

21. Millions of children and teens lose access to accounts as Australia's world-first social media ban begins. URL: https://www.theguardian.com/australia-news/2025/dec/09/australia-under-16-social-media-ban-begins-apps-listed

22. Regulation (EU) 2021/784 of the European Parliament and of the Council of 29.04.2021 on addressing the dissemination of terrorist content online. 17.05.2021. URL: https://eur-lex.europa.eu/eli/reg/2021/784/oj/eng.

23. Проект Закону про внесення змін до деяких законів України щодо регулювання діяльності платформ спільного доступу до інформації, через які поширюється масова інформація від 25.03.2024 №11115. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/43884.

Олександр Миколайович Поляков
начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
03113, вул. Миколи Василенка,3, Київ, Україна
email: hortytca@gmail.com

Oleksandr M. Poliakov
Head of the Department, Ukrainian Scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine
03113, Kyiv Ukraine, M. Vasylenka Str. 3
email: hortytca@gmail.com

Рекомендоване цитування: Поляков О.М. Загрозливі тенденції поширення терористичного контенту в мережі Інтернет та пропаганди тероризму. *Інформація і право.* № 2(57)/2026. 2026. С. 238-250. https://doi.org/10.37750/2616-6798.2026.2(57).364488
Suggested Citation: Poliakov O. (2026) Dangerous Trends in the Spread of Terrorist Content on the Internet and Terrorist Propaganda. *Information and Law*. 2(57)/2026. 238-250. https://doi.org/10.37750/2616-6798.2026.2(57).364488

Дата надходження статті до редакції: 15.04.2026 р.
Дата прийняття статті до друку після рецензування: 05.05.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~