УДК: 004.056:351.746.1:316.334.56 *DOI: https://doi.org/10.32631/vca.2024.3.74*

Віктор Михайлович ВАСИЛЕНКО,
доктор юридичних наук, доцент
(Харківський національний університет внутрішніх справ, м. Харків)

РОЛЬ ГРОМАД У ЗАБЕЗПЕЧЕННІ ЦИФРОВОЇ БЕЗПЕКИ: ПАРТНЕРСТВО З ПОЛІЦІЄЮ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Стрімке зростання впливу цифрових технологій на всі сфери життя суспільства супроводжується збільшенням кількості гібридних загроз, які поєднують елементи кіберзлочинності, інформаційного впливу, соціальної інженерії та маніпуляцій у медіапросторі. В умовах війни, політичної турбулентності та інформаційної вразливості українського суспільства питання цифрової безпеки набуває особливої актуальності. Територіальні громади, як основа децентралізації, виступають не лише адміністративними одиницями, а й активними учасниками побудови національної стійкості до сучасних загроз. У межах дослідження розкрито потенціал громад у виявленні кіберзагроз, фіксації ознак дезінформації та протидії поширенню фейкових кампаній. Зазначено, що найбільш ефективною моделлю реагування є системна співпраця між громадами та правоохоронними структурами, яка передбачає не лише обмін інформацією, а й створення спільних локальних ініціатив у сфері цифрової освіти, моніторингу онлайн-простору та розбудови інформаційної грамотності. Особливу увагу приділено формуванню цифрової культури як ключової умови підвищення рівня колективної обізнаності й відповідальності. Представлено приклади створення місцевих центрів цифрової безпеки, молодіжних хабів, онлайн-платформ для верифікації інформації та освітніх проєктів, спрямованих на розвиток критичного мислення. Підкреслено, що сталий розвиток безпечного цифрового середовища на місцевому рівні є передумовою забезпечення національної безпеки в умовах гібридного протистояння. Запропоновано бачення громад як рівноправних партнерів держави в побудові стійкої цифрової екосистеми.

Ключові слова: *цифрова безпека, гібридні загрози, територіальні громади, дезінформація, партнерство з поліцією, цифрова культура, інформаційна стійкість, кібербезпека, медіаграмотність, цифрова освіта.*

Постановка проблеми. У контексті зростання масштабів гібридних загроз, що охоплюють кіберзлочинність, дезінформацію, психологічний тиск і технологічні маніпуляції, питання цифрової безпеки набуває пріоритетного значення не лише на державному, а й на локальному рівні. Територіальні громади, як осередки життєдіяльності населення, дедалі частіше стають об'єктами цілеспрямованих атак у цифровому просторі. Водночас відсутність належного рівня цифрової культури, обмежений доступ до якісної цифрової освіти та низька медіаграмотність мешканців громад створюють сприятливий ґрунт для поширення фейкових повідомлень, соціальних маніпуляцій і недовіри до державних інституцій. Особливу складність становить відсутність сталої моделі співпраці між громадами та органами правопорядку щодо моніторингу, виявлення й оперативного реагування на цифрові загрози. У багатьох випадках поліція не має достатнього ресурсу або локального контексту для швидкої і точкової протидії інформаційним загрозам, тоді як громади залишаються поза межами формалізованих механізмів кіберзахисту. Водночас взаємодія між цими двома структурами могла б стати ефективним інструментом формування системи локальної цифрової безпеки, що враховує специфіку конкретної території та потреби населення. Складність проблеми посилюється швидкою трансформацією самих загроз – від примітивних шахрайських схем до добре скоординованих інформаційних операцій, що мають політичні або соціально-дестабілізаційні цілі. В умовах таких викликів ключовим завданням стає розроблення механізмів залучення громад до активної участі в забезпеченні цифрової безпеки, включно зі створенням інструментів партнерства з поліцією, ініціюванням освітніх та моніторингових проєктів, а також формуванням цифрової культури як основи інформаційної стійкості. Вирішення цієї проблеми потребує системного, міждисциплінарного підходу, адаптації безпекової політики до нових реалій та поглиблення міжінституційної взаємодії на рівні громада – поліція – держава.

У контексті зростання актуальності цифрової безпеки на тлі гібридної війни, що ведеться проти України, окремі аспекти цієї тематики були розглянуті в працях низки українських науковців. Зокрема, С. О. Петренко досліджував особливості дезінформаційного впливу на місцеві спільноти та виокремлював загрози, пов'язані з маніпулятивними наративами в соціальних мережах. У своїй роботі автор підкреслює, що ефективна протидія фейковим кампаніям неможлива без активного залучення локального рівня.

Роль територіальних громад у системі національної безпеки аналізувала І. В. Коваленко, приділяючи увагу питанням децентралізації та розвитку безпекових ініціатив на місцях. Дослідниця наголошує на важливості взаємодії між місцевою владою, громадськими організаціями та

представниками правоохоронних структур.

У своїх публікаціях Л. М. Дмитренко порушує проблему цифрової грамотності населення як одного з головних чинників інформаційної вразливості громад. Особливий акцент зроблено на просвітницьких кампаніях і розвитку цифрової культури як інструменту протидії гібридним впливам.

У межах дослідження правоохоронної діяльності в умовах новітніх викликів А. Г. Мельник вивчав потенціал *community policing* у зміцненні довіри до поліції та залученні громад до процесів превентивної безпеки. Його праці демонструють, що сучасна поліція потребує партнерських форматів взаємодії з населенням, зокрема в цифровому просторі.

Варто відзначити дослідження Н. Ю. Шевченко, яка розглядала практичні аспекти кібербезпеки в умовах децентралізації. Авторка акцентує увагу на нерівномірності рівня цифрової підготовки в громадах і необхідності створення локальних інституцій цифрового захисту за участю поліції, волонтерів та освітян.

Тим часом попри наявність окремих напрацювань, системного підходу до аналізу партнерства громад і поліції у сфері цифрової безпеки в умовах гібридних загроз у вітчизняній науці наразі не сформовано. Це свідчить про існування наукової лакуни, заповнення якої є важливою умовою для формування ефективної державної та локальної політики безпеки. У цьому контексті зроблена спроба визначити концептуальні підходи до розуміння ролі громад у цифровій безпеці, виявити чинники, що зумовлюють рівень їхньої участі у протидії кіберзагрозам, а також дослідити практичні моделі співпраці громад із поліцією. Основну увагу приділено аналізу потенціалу громад як джерела ініціатив у сфері цифрової освіти, моніторингу інформаційного простору, формування цифрової культури та впровадження превентивних заходів у співпраці з правоохоронними структурами. У межах дослідження також передбачено аналіз чинного стану нормативно-правового забезпечення, можливостей міжсекторної взаємодії та рівня підготовленості органів місцевого самоврядування до реагування на гібридні загрози. Серед іншого, дослідження також охоплює розроблення пропозицій щодо оптимізації комунікаційної моделі взаємодії поліції та громадськості у сфері цифрової безпеки, формування локальних політик у галузі кіберзахисту, розвиток практик підвищення обізнаності населення та активізацію соціального капіталу громад у безпековому вимірі. Особливий акцент зроблено на потребі побудови горизонтальних механізмів взаємодії, за яких громади не виступають об’єктами захисту, а стають суб’єктами цифрової безпеки, здатними до самозахисту, спостереження, аналізу й дій.

Таким чином, проведене дослідження створить наукове підґрунтя для формування нової моделі цифрової безпеки, що базується на партнерстві громад і поліції, враховує локальний контекст, специфіку гібридних загроз і потенціал розвитку цифрової культури як ключового елементу інформаційної стійкості.

Метою статті є комплексне дослідження ролі територіальних

громад у забезпеченні цифрової безпеки в умовах гібридних загроз, а також обґрунтування доцільності та ефективності партнерства між громадами і правоохоронними органами як інструменту формування стійкого локального цифрового середовища.

Виклад основного матеріалу. У сучасному безпековому контексті, який характеризується ескалацією інформаційної війни, кібератак, поширенням фейків, маніпулятивних наративів і дезінформаційних кампаній, особливої актуальності набуває залучення місцевих суб'єктів до процесів цифрового захисту. Гібридна агресія, що поєднує традиційні та новітні методи впливу, демонструє високу ефективність саме на рівні локальних спільнот, де низький рівень обізнаності, фрагментована інформаційна політика та відсутність сталих механізмів реагування створюють підґрунтя для поширення загроз.

Цифрова безпека у XXI ст. перетворилася на одну з провідних складових загальнонаціональної безпеки держав, які перебувають у стані перманентних інформаційних, політичних, військових і економічних викликів. Стрімкий розвиток інформаційно-комунікаційних технологій суттєво змінив характер сучасних загроз, надавши їм нових форм – невидимих, швидких, адаптивних. У наш час кібератаки, поширення дезінформації, маніпулятивні медіакампанії та порушення роботи цифрової інфраструктури стали звичними інструментами гібридної війни. Особливо гостро ці процеси проявляються в умовах затяжного воєнного конфлікту та посилення міжнародного тиску, де інформаційна сфера відіграє роль не лише простору обміну знаннями, а й арени стратегічного протистояння. Гібридні загрози, які поєднують як традиційні (військові, економічні, політичні), так і нетрадиційні (інформаційні, кібернетичні, психологічні) форми впливу, дедалі частіше спрямовані не лише проти державних структур, а й на дестабілізацію місцевого середовища, підрив суспільної довіри, розкол соціального простору та дискредитацію інституцій публічної влади. У таких умовах постає об'єктивна необхідність не лише оновлення державної політики у сфері цифрової безпеки, а й мобілізації потенціалу місцевих громад, які є найближчими до населення та першими зіштовхуються з наслідками цифрових інцидентів. Територіальні громади відіграють ключову роль у виявленні, моніторингу та локальному реагуванні на інформаційно-комунікаційні загрози. Їхнє залучення до системи цифрової безпеки не повинно обмежуватися лише функціями спостереження або отримання інформації від центру. Навпаки, громади мають стати повноцінними суб'єктами національного захисту в цифровому просторі Їхній потенціал полягає не лише в географічній наближеності до проблем, а й у здатності до швидкої мобілізації людських і соціальних ресурсів, реалізації просвітницьких ініціатив, розвитку цифрової освіти, створення волонтерських хабів, центрів допомоги, моніторингових груп та інших локальних рішень. Одним із найважливіших інструментів забезпечення ефективної безпеки на рівні громади є налагодження партнерства з правоохоронними органами, зокрема з підрозділами

Національної поліції. Така співпраця дає змогу перейти від реактивної моделі до проактивної, що охоплює профілактику кіберзлочинності, попередження поширення фейкових повідомлень, розпізнавання ворожих інформаційних впливів, а також формування інформаційної грамотності серед населення. Формат взаємодії «громада – поліція» передбачає обмін знаннями, проведення тренінгів, спільне реагування на інциденти, створення локальних систем кіберспостереження, впровадження інформаційних кампаній і підтримку цифрової освіти. У дослідженні питання цифрової безпеки на рівні територіальних громад важливо зосередити увагу на пошуку ефективних моделей партнерства, аналізі наявних ініціатив, бар'єрів і потенціалу для їхнього розвитку в умовах обмежених ресурсів і зростаючих викликів.

Гібридні загрози становлять новий тип багатовекторного впливу, що поєднує кібернетичні атаки, інформаційні маніпуляції, психологічні операції, економічний тиск і використання внутрішніх соціальних конфліктів. Їхня головна мета полягає не стільки в прямій конфронтації, скільки в поступовому розхитуванні цілісності держави, зниженні рівня громадської довіри, створенні атмосфери дестабілізації. Особливо уразливими до такого впливу залишаються місцеві громади, які є точкою входу для багатьох гібридних інструментів впливу, зокрема дезінформації, соціальних провокацій і технологічних атак на локальні інфраструктурні об'єкти. На локальному рівні гібридні загрози проявляються у різних формах. Однією з найчастіших форм є поширення неправдивої інформації через соціальні мережі та месенджери[1]. Такі повідомлення можуть містити відверті фейки, емоційні маніпуляції або спотворені факти, спрямовані на посилення соціальної напруги, дискредитацію місцевої влади чи деморалізацію населення. Уразливість громад до подібних інформаційних атак зумовлена низьким рівнем медіаграмотності, нерівномірним доступом до достовірних джерел інформації, а також браком навичок критичного сприйняття цифрового контенту[2]. Окремим вектором є кібератаки на локальні адміністративні системи, освітні портали, сайти комунальних служб і навіть особисті акаунти представників місцевої влади. Такі дії зазвичай не мають миттєвого катастрофічного ефекту, але поступово підривають довіру громадян до функціонування інституцій, викликають паніку й формують відчуття хаосу. Атаки на інформаційну безпеку супроводжуються поширенням чуток, провокаційних повідомлень, а також активною діяльністю бот-мереж, спрямованою на формування штучного консенсусу навколо деструктивних меседжів. Варто також виокремити психологічний вимір гібридного впливу, що проявляється через створення

[1] Володько В. О. Актуальні питання розробки, впровадження і використання компонентів інформаційних технологій в діяльності правоохоронних органів. *Застосування інформаційних технологій у правоохоронній діяльності* : матеріали круглого столу (м. Харків, 14 груд. 2023 р.) / МВС України, Харк. нац. ун-т внутр. справ, Ф-т № 6, Каф. кібербезпеки та DATA-технологій. Харків : ХНУВС, 2023. С. 84.

[2] Вольнова Л. М., Камінська А. О., Ляска О. П. Вплив соціальних мереж на психічне здоров'я сучасної молоді. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. *Серія: Психологія.* 2023. Т. 34 (73). № 6. С. 4.

відчуття постійної загрози, невизначеності та втрати контролю[1]. Це особливо небезпечно в умовах кризових ситуацій, зокрема під час військових дій або надзвичайних ситуацій, коли громади стають основною ціллю інформаційного тиску. Страх, невпевненість, втома від напруги – це ґрунт, на якому активно проростають ворожі інформаційні наративи.

Попри складність і багатогранність проблеми, саме громади мають потенціал стати першою лінією оборони у сфері цифрової безпеки. Їхня здатність до самоорганізації, територіальна наближеність до жителів, налагоджені горизонтальні зв'язки та розуміння локального контексту відкривають можливості для оперативного реагування на прояви гібридного впливу. Однак реалізація цього потенціалу потребує системної підтримки з боку держави, інвестицій у цифрову освіту, створення механізмів взаємодії з поліцією та іншими суб'єктами безпеки. Формування цифрової компетентності громади, запровадження локального моніторингу інформаційного середовища, підтримка ініціатив із розвитку критичного мислення – усе це має стати невід'ємною частиною нової безпекової архітектури на місцевому рівні.

Партнерство між територіальними громадами та поліцією у сфері цифрової безпеки є стратегічно важливим інструментом зміцнення стійкості до гібридних загроз. У сучасних умовах, коли цифрові атаки та інформаційні маніпуляції спрямовані не лише проти національних інституцій, а й безпосередньо на місцеві спільноти, ефективна взаємодія між правоохоронними органами й громадянами стає нагальною потребою[2]. Така співпраця передбачає не лише формальну координацію дій, а передусім побудову довіри, обмін знаннями та взаємну підтримку у сфері виявлення й запобігання загрозам у цифровому середовищі. Поліція, з огляду на свою інституційну спроможність і правовий мандат, може виконувати не лише функцію реагування, а й активно долучатися до просвітницької та профілактичної роботи. Одним із ключових аспектів партнерства є спільна організація освітніх заходів для мешканців громад. Йдеться про тренінги з основ цифрової безпеки, майстер-класи з розпізнавання дезінформації, зустрічі з фахівцями кіберполіції, під час яких обговорюються реальні кейси, що сталися в межах громади[3]. Це дозволяє не лише підвищити рівень обізнаності населення, а й формувати довіру до правоохоронців як до відкритого та доступного партнера.

---

[1] Грачов Є. О. До проблеми визначення чинників, що впливають на стан діджиталізації сфери надання адміністративних послуг в сучасних умовах. *Теоретичні питання юриспруденції і проблеми правозастосування: виклики XXI століття :* тези доп. учасників VII Всеукр. наук.-практ. конф. (Харків, 09 черв. 2023 р.) ; Наук.-дослід. ін-т публ. політики і соц. наук. Харків: НДІ ППСН, 2023. С. 27.

[2] Зінченко Д. А. Стратегія боротьби з кіберзлочинністю в умовах глобалізації інформаційних просторів. *Застосування інформаційних технологій у правоохоронній діяльності* : матеріали круглого столу (м. Харків, 14 груд. 2023 р.) / МВС України, Харк. нац. ун-т внутр. справ, Ф-т № 6, Каф. кібербезпеки та DATA-технологій. Харків : ХНУВС, 2023 С. 106.

[3] Зінченко Д. А., Макарова О. П. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». Вінниця : ХНУВС, 2023. С. 119.

Досвід окремих громад свідчить про ефективність створення ініціативних груп, до складу яких входять місцеві активісти, освітяни, молодь і представники поліції. Такі формати дають змогу оперативно реагувати на загрози, здійснювати моніторинг інформаційного простору, виявляти ознаки деструктивної активності та вчасно інформувати відповідні структури. Особливого значення набуває участь молоді, яка володіє високим рівнем цифрових навичок і часто є першою ціллю інформаційних впливів[1]. Її залучення до превентивних ініціатив сприяє формуванню відповідального ставлення до цифрового середовища та поширенню навичок цифрової гігієни серед однолітків. Одним із перспективних напрямів є впровадження локальних програм цифрового менторства, у межах яких досвідчені фахівці спільно з правоохоронцями навчають громаду способів захисту особистих даних, безпечного користування соціальними мережами, протидії фішингу та онлайн-шахрайству. Такі програми можуть функціонувати на базі бібліотек, освітніх закладів, центрів надання адміністративних послуг або хабів цифрової освіти. Крім того, партнерство з поліцією дає змогу залучити фахівців до розроблення локальних стратегій цифрової безпеки, що враховують специфіку конкретної громади, її технічні можливості, демографічну структуру, рівень цифрової грамотності та прецеденти загроз. Варто також ураховувати, що успішна співпраця потребує двосторонньої ініціативи. З боку поліції важливо демонструвати відкритість, забезпечувати регулярну комунікацію, оперативно реагувати на сигнали від громади, виявляти гнучкість у виборі форм взаємодії. З боку громади необхідно ініціювати діалог, проявляти активність у навчанні, формувати внутрішні структури самоорганізації. Такий підхід дає змогу створити сталу інфраструктуру цифрової безпеки на рівні громади, яка не залежить винятково від зовнішніх ресурсів.

Вважаємо, що формування ефективного партнерства між поліцією та громадою у сфері цифрової безпеки є передумовою створення нової моделі локального захисту, у якій населення не виступає пасивним об’єктом впливу, а стає активним учасником процесів запобігання, навчання та реагування на загрози. Це відповідає сучасним підходам до безпеки як спільної відповідальності, що забезпечується через довіру, співпрацю та спільне знання.

Цифрова культура на рівні місцевих громад розглядається як один із ключових чинників формування інформаційної стійкості в умовах постійного впливу гібридних загроз. Вона охоплює не лише технічну обізнаність щодо правил безпечного користування цифровими технологіями, а й здатність критично оцінювати інформацію, розуміти механізми маніпуляцій, орієнтуватися в етичних нормах поведінки у

[1] Колісник Т. П. Цифрова трансформація системи Міністерства внутрішніх справ України на період до 2023 року. *Протидія кіберзлочинності та торгівлі людьми :* зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 27 трав. 2022 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека»; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2022. С. 48.

віртуальному просторі[1]. У сучасному суспільстві, де значна частина комунікації, соціальної взаємодії та ухвалення рішень відбувається онлайн, питання розвитку цифрової культури стає основою для побудови захищеного середовища.

Територіальні громади мають потенціал стати каталізаторами змін у цьому напрямі, особливо завдяки безпосередній близькості до людей, гнучкості в ухваленні рішень і можливості впроваджувати адаптовані освітні формати. Місцеві ініціативи можуть охоплювати різні вікові й соціальні групи, враховувати їхні особливості та рівень цифрових компетенцій. Практика показує, що найефективнішими є ті проєкти, які поєднують навчання з практичною діяльністю, створюють умови для взаємодії різних поколінь і формують спільну відповідальність за інформаційну безпеку[2]. Особливу роль у розвитку цифрової культури відіграють молодіжні ініціативи, стартапи, технохаби та волонтерські осередки. Молодь, як найбільш активна та технічно підготовлена частина суспільства, має потенціал стати рушієм змін: транслювати позитивні цифрові практики, створювати якісний контент, викривати фейки та прояви ворожої пропаганди. Успішні приклади свідчать, що саме молодіжні платформи часто стають першими індикаторами появи маніпулятивних інформаційних кампаній, адже вони реагують швидко, гнучко та креативно. Розвитку цифрової культури також сприяє тісна взаємодія громад з правоохоронними органами. Залучення представників поліції до навчального процесу дає змогу формувати розуміння реальних загроз, що можуть виникнути в цифровому просторі[3]. Водночас це сприяє зміцненню довіри до інституцій, коли мешканці громади відчувають реальну підтримку та зацікавленість з боку держави в їхній інформаційній безпеці. Формат спільних просвітницьких заходів, інтерактивних зустрічей, форумів чи інформаційних кампаній підвищує рівень залученості та створює простір для міжсекторального діалогу. Ще одним важливим аспектом є створення освітніх платформ, які діють постійно та дають змогу формувати навички поступово, з урахуванням змін у технологіях та нових викликів, а не одноразово[4]. Громади можуть ініціювати відкриті лекції, консультаційні центри, онлайн-курси з медіаграмотності, адаптовані для різних аудиторій – від школярів до людей похилого віку. Такий підхід дає змогу уникнути

[1] Литвинов О. М. Діджиталізація: на порозі цифрового дахау. *Держава і злочинність. Нові виклики в епоху постмодерну* : зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора О. М. Литвака (м. Харків, 23 квіт. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків : ХНУВС, 2020. С. 171.

[2] Наджафлі Е. Цифрова держава в контексті правової реформи в Україні : теоретико-правовий аспект. *Право і безпека.* 2022. № 2 (85). С. 205.

[3] Нестеров Д. С. Роль сучасних інформаційних технологій та цифрової безпеки у забезпеченні стабільності та процвітання суспільства та держави. *Наука в умовах воєнного стану: пошуки, проблеми, перспективи розвитку:* матер. Всеукр. наук.-практ. конф. молодих вчених (м. Дніпро, 3 трав. 2023 р.) / МВС України, Дніпропетров. держ. ун-т внутр. справ. Дніпро : ДДУВС, 2023. С. 248.

[4] Расторгуєва Н. О., Загуменна Ю. О. Діджиталізація сучасного суспільства. *Протидія кіберзагрозам та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 26 листоп. 2019 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проєктів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 131.

поверхневого навчання та створити сталу систему цифрової просвіти на місцях.

На нашу думку, цифрова культура в громаді – це не лише набір навичок, а й складова колективної ідентичності, що ґрунтується на відповідальності, солідарності та повазі до інформаційного простору. Її розвиток є фундаментом для формування громад, здатних не лише реагувати на інформаційні загрози, а й діяти на випередження, створюючи навколо себе безпечне, освічене та адаптивне цифрове середовище. Саме через посилення цього культурного виміру громади поступово переходять від ролі об'єкта інформаційного впливу до активного суб'єкта цифрової трансформації.

Підсумовуючи вищевикладене, можемо зробити висновок, що забезпечення цифрової безпеки в умовах гібридних загроз вимагає переосмислення ролі територіальних громад як активних учасників у побудові нової системи безпеки, орієнтованої на локальний контекст, швидке реагування та соціальну відповідальність. Сучасна практика доводить, що централізованих зусиль держави недостатньо для ефективної протидії динамічним і багатоформатним викликам у цифровому середовищі. Саме громади завдяки своїй територіальній наближеності до проблем, високому рівню взаємодії між учасниками локального середовища та здатності до гнучкої самоорганізації можуть стати ключовими осередками превентивного впливу. Вони мають потенціал не лише виявляти деструктивні цифрові явища на ранніх етапах, а й формувати навколо себе простір критичного мислення, взаємодії, солідарності та обміну знаннями. Окремої уваги заслуговує партнерство громад із правоохоронними органами як важлива складова нової парадигми цифрової безпеки. Поліція, що сприймається не як репресивна структура, а як учасник діалогу, наставник і партнер, здатна істотно впливати на рівень цифрової стійкості громад. В умовах гібридної війни така модель співпраці дозволяє не лише реагувати на загрози, а й працювати на випередження через спільні освітні ініціативи, публічні кампанії з підвищення кіберграмотності, створення аналітичних і моніторингових груп, підтримку молодіжних ініціатив та волонтерських рухів. Довіра, прозорість комунікацій, залучення до процесу ухвалення рішень стають важливими елементами формування безпечного цифрового середовища. Важливу роль у зміцненні інформаційної стійкості відіграє формування цифрової культури як нової соціальної норми. Громади, які розвивають компетенції у сфері цифрової освіти, медіаграмотності, етичного користування інформаційними ресурсами, стають менш вразливими до зовнішніх впливів. Це не лише підвищує рівень захищеності окремих громадян, а й створює середовище, у якому фейки, дезінформація, цифрові маніпуляції не мають живильного ґрунту для поширення. Підтримка таких процесів на інституційному рівні, зокрема через муніципальні програми, державно-громадські партнерства та міжсекторну взаємодію, є критично важливою умовою національної безпеки.

З огляду на вищезазначене, можемо констатувати, що майбутнє цифрової безпеки лежить у площині розвитку горизонтальних зв'язків, посилення локальної спроможності громад, підтримки їхнього освітнього, технічного та аналітичного потенціалу. Саме ці фактори мають визначати ефективність захисту суспільства в умовах швидкозмінних викликів, притаманних гібридним загрозам. Формування спільної відповідальності за цифрове середовище, розвиток культури співпраці та безперервне навчання стають визначальними орієнтирами в побудові стійкої цифрової екосистеми.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Володько В. О. Актуальні питання розробки, впровадження і використання компонентів інформаційних технологій в діяльності правоохоронних органів. *Застосування інформаційних технологій у правоохоронній діяльності* : матеріали круглого столу (м. Харків, 14 груд. 2023 р.) / МВС України, Харк. нац. ун-т внутр. справ, Ф-т № 6, Каф. кібербезпеки та DATA-технологій. Харків : ХНУВС, 2023. С. 80–85.

2. Вольнова Л. М., Камінська А. О., Ляска О. П. Вплив соціальних мереж на психічне здоров'я сучасної молоді. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. *Серія: Психологія.* 2023. Т. 34 (73). № 6. С. 1–5. DOI: https://doi.org/10.32782/2709-3093/2023.6/01.

3. Грачов Є. О. До проблеми визначення чинників, що впливають на стан діджиталізації сфери надання адміністративних послуг в сучасних умовах. *Теоретичні питання юриспруденції і проблеми правозастосування: виклики XXI століття :* тези доп. учасників VII Всеукр. наук.-практ. конф. (Харків, 09 черв. 2023 р.) ; Наук.-дослід. ін-т публ. політики і соц. наук. Харків: НДІ ППСН, 2023. С. 29–30.

4. Зінченко Д. А. Стратегія боротьби з кіберзлочинністю в умовах глобалізації інформаційних просторів. *Застосування інформаційних технологій у правоохоронній діяльності* : матеріали круглого столу (м. Харків, 14 груд. 2023 р.) / МВС України, Харк. нац. ун-т внутр. справ, Ф-т № 6, Каф. кібербезпеки та DATA-технологій. Харків : ХНУВС, 2023 С. 105–107.

5. Зінченко Д. А., Макарова О. П. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». Вінниця : ХНУВС, 2023. С. 118–121.

6. Колісник Т. П. Цифрова трансформація системи Міністерства внутрішніх справ України на період до 2023 року. *Протидія кіберзлочинності та торгівлі людьми :* зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 27 трав. 2022 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека»; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2022.С. 48–49.

7. Литвинов О. М. Діджиталізація: на порозі цифрового дахау. *Держава і злочинність. Нові виклики в епоху постмодерну* : зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора О. М. Литвака (м. Харків, 23 квіт. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків : ХНУВС, 2020. С. 170–172.

8. Наджафлі Е. Цифрова держава в контексті правової реформи в Україні: теоретико-правовий аспект. *Право і безпека.* 2022. № 2 (85). С. 202–217. DOI: https://doi.org/10.32631/pb.2022.2.19.

9. Нестеров Д. С. Роль сучасних інформаційних технологій та цифрової безпеки у забезпеченні стабільності та процвітання суспільства та держави. *Наука в умовах воєнного стану: пошуки, проблеми, перспективи розвитку:* матер. Всеукр. наук.-практ. конф. молодих вчених (м. Дніпро, 3 трав. 2023 р.) / МВС України, Дніпропетров. держ. ун-т внутр. справ. Дніпро : ДДУВС, 2023. С. 248–249.

10. Расторгуєва Н. О., Загуменна Ю. О. Діджиталізація сучасного суспільства. *Протидія кіберзагрозам та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 26 листоп. 2019 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проєктів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 130–132.

Стаття надійшла до редакції 09.11.2024

Viktor M. VASYLENKO,
Doctor of Science in Law, Associate Professor
(Kharkiv National University of Internal Affairs, Kharkiv, Ukraine)

THE ROLE OF COMMUNITIES IN ENSURING DIGITAL SECURITY: PARTNERSHIP WITH THE POLICE IN THE FACE OF HYBRID THREATS

The rapid expansion of digital technologies across all spheres of society is accompanied by a growing number of hybrid threats, combining elements of cybercrime, informational influence, social engineering, and manipulation in the media space. In the context of war, political turbulence, and the informational vulnerability of Ukrainian society, the issue of digital security has become particularly urgent. Territorial communities, as the foundation of decentralization, act not only as administrative units but also as active participants in building national resilience to contemporary threats. This study explores the potential of communities in detecting cyber threats, identifying signs of disinformation, and countering the spread of fake campaigns. The most effective response model is highlighted as systematic cooperation between communities and law enforcement agencies, which includes not only the exchange of information but also the creation of joint local initiatives in the fields of digital education, online monitoring, and the development of informational literacy. Special attention is given to the formation of digital culture as a key condition for increasing collective awareness and responsibility. Examples are provided of the

establishment of local digital security centers, youth hubs, online platforms for information verification, and educational projects aimed at enhancing critical thinking. Sustainable development of a secure digital environment at the local level is emphasized as a prerequisite for ensuring national security under conditions of hybrid confrontation. The article proposes a vision of communities as equal partners of the state in building a resilient digital ecosystem.

Keywords: *digital security, hybrid threats, territorial communities, disinformation, police partnership, digital culture, information resilience, cybersecurity, media literacy, digital education.*