ISSN 2220-8089 Вісник Харківського національного університету імені В. Н. Каразіна, серія «Питання політології», 2025, випуск 47

https://doi.org/10.26565/2220-8089-2025-47-06
УДК 351.86:004.056]:316.658.4(477.54)
Олександра Ігорівна Зінченко
Аспірантка кафедри політології філософського факультету Харківського національного університету ім. В.Н. Каразіна, майдан Свободи, 4, 61022, м. Харків
alekca.98@ukr.net, https://orcid.org/0000-0003-1623-957X

КІБЕРБЕЗПЕКА ЯК ЕЛЕМЕНТ ДЕМОКРАТИЧНОЇ КОНСОЛІДАЦІЇ: УРОКИ ХАРКІВЩИНИ

В умовах гібридної війни та цілеспрямованої інформаційної агресії проблема кібербезпеки набуває особливої ваги не лише як технічне завдання, а і як ключовий чинник забезпечення національної, політичної та соціальної стійкості. Кібербезпека постає як важливий елемент демократичного розвитку, адже інформаційні атаки часто спрямовані на підрив суспільної довіри, дестабілізацію місцевого управління та знецінення демократичних інституцій. Розглядається досвід України, а саме Харківської області в якості значного прикладу, як регіональні спільноти можуть протистояти складним викликам кібернетичного та інформаційного характеру. На прикладі Харківщини простежується не лише технічне, а й чітко виражене політичне забарвлення кіберзагроз, а саме: масові DDoS-атаки на державні сервіси, злам інформаційних ресурсів, кампанії фішингу, шпигунські програми, атаки на місцеві медіа, активне використання ботоферм у соціальних мережах, тобто усе, що виступає інструментом тиску на громадську думку, створення паніки, дискредитації органів місцевого самоврядування та поширення дезінформації.

Підкреслюється особлива небезпечність інформаційних кампаній, які маскуються під легітимні джерела, але мають на меті поширення наративів ворожої пропаганди, зниження рівня критичного мислення та формування ворожого до демократичних цінностей середовища. Ці кіберінструменти можуть бути спрямовані як на підрив виборчого процесу, так і на створення штучного невдоволення серед населення. Водночас, приклад Харківської області демонструє, що за умови належної координації між органами влади, силовими структурами, медіа та громадянським суспільством можливе ефективне протистояння кіберзагрозам. Робиться висновок, що підвищення рівня цифрової грамотності населення, розбудова локальних систем кіберзахисту, інформаційна прозорість та залучення громадян до протидії дезінформації сприяють формуванню стійкої демократії.

Ключові слова: *кібербезпека, демократична консолідація, інформаційні операції, громадська стійкість, ботоферми, регіональна безпека*.

Як цитувати: Зінченко, О.І. 2025. Кібербезпека як елемент демократичної консолідації: уроки Харківщини. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Питання політології»* 47: 46-52. https://doi.org/10.26565/2220-8089-2025-47-06

In cites: Zinchenko, Oleksandra. 2025. Cybersecurity as an Element of Democratic Consolidation: Lessons From Kharkiv Region. *The Journal of V. N. Karazin Kharkiv National University. Series «Issues of Political Science»* 47: 46-52. https://doi.org/10.26565/2220-8089-2025-47-06 (in Ukrainian)

ISSN 2220-8089 Вісник Харківського національного університету імені В. Н. Каразіна, серія «Питання політології», 2025, випуск 47

Кіберпростір став одним із ключових вимірів сучасного суспільного життя. Інформаційні технології проникають у всі сфери діяльності – від державного управління і бізнесу до особистого спілкування громадян. Особливо важливе місце кіберпростір займає в демократичних суспільствах, де свобода доступу до інформації, відкритість влади та активність громадян є фундаментальними цінностями. Водночас ці цінності роблять демократії вразливими до кіберзагроз, адже кіберпростір може бути використаний як інструмент маніпуляції громадською думкою, втручання у виборчі процеси, дезінформації та навіть паралізації критично важливих інфраструктур.

Для України це питання набуло особливого значення в умовах демократичної трансформації та тривалої війни, яку Росія веде не лише на полі бою, а й в інформаційному просторі. З початку повномасштабного вторгнення у 2022 році Україна стала мішенню тисяч кібератак, спрямованих на державні органи, енергетичні системи, медіа та громадські організації. Ці атаки мали на меті дестабілізувати внутрішню ситуацію, посіяти паніку, підірвати довіру громадян до влади та демократичних процедур (Дубов 2013: 120).

Кібербезпека в таких умовах перетворилася не лише на технічне завдання, а й на стратегічний чинник національної безпеки та демократичної консолідації. Вона забезпечує захист права громадян на правдиву інформацію, гарантує безпечне функціонування державних і місцевих органів, сприяє прозорості виборів, а також зберігає стабільність суспільства в умовах гібридної війни. Ефективна кібербезпека зміцнює довіру людей до демократичних інституцій, адже безпека інформаційного простору є запорукою справедливості, відкритості та підзвітності влади.

Особливу роль відіграє регіональний рівень. Харківщина як прикордонна область з початку війни стала однією з головних мішеней ворожих кібератак і інформаційних операцій. Її досвід виявився показовим для всієї країни, оскільки саме тут демократичні механізми, громадська активність та системи кіберзахисту проходять випробування в екстремальних умовах. Уроки Харківщини демонструють, наскільки важливо поєднувати технологічний захист, інформаційну грамотність населення та активну участь громадян у збереженні інформаційної безпеки як складової демократичного розвитку країни (Бухарєв 2018).

Поширеним типом загроз стали фішингові атаки (phishing) – масове надсилання фальшивих електронних листів, нібито від імені офіційних структур, органів влади, правоохоронних відомств або благодійних організацій. Такі листи містили посилання на підроблені сайти, які імітували зовнішній вигляд справжніх ресурсів, з метою збору особистих даних, облікових записів, паролів, платіжної інформації або для завантаження шкідливого програмного забезпечення. Особливо активно такі атаки здійснювались у моменти оголошення гуманітарної допомоги, надання компенсацій або під час проведення виборів до органів місцевого самоврядування на деокупованих територіях. Зафіксовані також випадки кібершпигунства – встановлення шкідливого програмного забезпечення на робочі комп’ютери посадових осіб органів влади та представників громадських організацій. Таке ПЗ дозволяло віддалено зчитувати документи, стежити за листуванням, відстежувати геолокацію і навіть перехоплювати відео з вебкамер. У більшості випадків цільовими атаками охоплювалися керівники районних військових адміністрацій, представники благодійних фондів та журналісти, які володіли важливою для противника інформацією (Корнієнко 2018).

Окремим і надзвичайно небезпечним напрямом кіберзагроз для Харківщини стали інформаційні операції – сплановані масові кампанії з поширення фейкових повідомлень та маніпулятивного контенту через інтернет, соціальні мережі, месенджери та навіть SMS-розсилки. Протягом 2022–2024 років зафіксовано численні випадки поширення неправдивих повідомлень про нібито підготовку до повної евакуації міста Харкова, падіння обласної військової адміністрації, здачу окремих районів чи поразку українських військ. Ці повідомлення системно з’являлися у критичні моменти – напередодні великих обстрілів, атак на об’єкти критичної інфраструктури або під час активізації бойових дій поблизу області. Метою таких кампаній було дестабілізувати соціально-політичну ситуацію в регіоні, спричинити паніку серед населення, підірвати довіру до місцевої влади та українських військових, створити враження хаосу і безконтрольності.

Велику роль у реалізації таких операцій відігравали ботоферми – мережі фейкових акаунтів, які автоматично поширювали панічні повідомлення у Facebook, Telegram, Instagram та TikTok. За допомогою

автоматизованих систем і тисяч ботів створювали штучне враження масового невдоволення, хаосу або вимагання «здати місто» для уникнення руйнувань. При цьому такі акаунти часто мали локалізовані назви, аватарки з українською символікою, і видавали себе за місцевих жителів, аби збільшити довіру до поширеного контенту (Макаренко 2011: 55).

Особливої небезпеки набули кібератаки на місцеві медіа, які під час війни стали одними з головних джерел оперативного інформування для населення Харківщини. Незалежні регіональні видання та інформаційні платформи регулярно зазнавали DDoS-атак, спрямованих на виведення їхніх сайтів з ладу під час кризових ситуацій. Також мали місце спроби зламу редакційних облікових записів у соцмережах і системах управління контентом. Мета таких атак – розмістити дезінформацію від імені авторитетних медіа, дискредитувати журналістів, поширити панічні чутки або неправдиві новини про ситуацію в місті та області.

У деяких випадках створювались фейкові сторінки-клони популярних місцевих медіа, які зовні повністю імітували справжні сайти, використовуючи схожі доменні імена, логотипи та дизайн. На цих ресурсах поширювалися фальшиві заяви обласної влади, сфабриковані «новини» про масову втечу керівництва області чи фейкові накази військового командування. Така тактика дозволяла швидко ввести в оману непідготовленого користувача, особливо в умовах обмеженого доступу до електроенергії, коли люди отримували інформацію переважно через смартфони в соцмережах і месенджерах.

Як зазначає В. Б. Дзюндзюк, інформаційна війна є невід'ємною частиною гібридної агресії, яка не обмежується лише військовими діями, а охоплює політичний, економічний, дипломатичний та інформаційний тиски на державу, її суспільство та інституції (Дзюндзюк 2018: 170). Такий багатовимірний характер конфлікту дозволяє агресору паралельно використовувати різні засоби впливу, підриваючи не лише мате-ріальну, а й морально-психологічну стійкість населення. Особливо ефективною ця стра-тегія стає тоді, коли військові дії супроводжуються активною кампанією дезінформації, поширенням фейкових повідомлень, маніпуляціями в соціальних мережах і кібер-атаками на важливі державні ресурси та медіа.

Це повною мірою стосується і Харківщини, яка з початку повномасштабного вторгнення Росії стала одним із найважливіших об'єктів ворожих інформаційно-психологічних операцій. Боротьба за контроль над регіональним інформаційним простором є не лише складовою загальної стратегії ворога щодо підриву демократичного порядку в Україні, а й спробою зруйнувати систему комунікації між владою та громадянами, дестабілізувати ситуацію в тилу та вплинути на ухвалення політичних рішень. В умовах війни інформаційна атака на місто чи область може мати не менш руйнівні наслідки, ніж військовий обстріл, оскільки масова паніка, поширення неправдивих новин або дискредитація влади можуть призвести до порушення громадського порядку, втрати довіри до керівних органів та ослаблення обороноздатності.

Д. В. Дубов також наголошує, що в умовах гібридної війни кібербезпека стає ключовою складовою національної безпеки, адже інформаційні технології дозволяють ворогу не лише впливати на громадську думку, а й безпосередньо втручатися у роботу державних органів, систем критичної інфраструктури, банківського сектору, медіапростору та цифрових сервісів (Дубов 2013: 120). Д. Дубов підкреслює, що саме регіональний досвід дозволяє глибше зрозуміти характер загроз та способи їх нейтралізації, оскільки на місцевому рівні найшвидше помітні наслідки інформаційних атак та ефективність заходів кіберзахисту. Харківщина, як регіон, що одночасно перебуває в зоні бойових дій і є важливим адміністративно-економічним центром, стала прикладом того, як локальні органи влади, ІТ-фахівці та громадськість можуть об'єднатися для протидії складним інформаційним загрозам.

За умов постійних кібератак, інформаційних вкидів і спроб дезорієнтації населення, інформаційна безпека перетворилася на один із головних чинників збереження довіри громадян до демократичних інституцій. Її значення особливо зросло в контексті організації виборів, проведення громадських слухань, роботи місцевих органів влади та функціонування цифрових сервісів електронного урядування. В умовах війни саме ці інститути стали основним каналом комунікації між громадянами та державою, забезпечуючи доступ до інформації про безпекову ситуацію, гуманітарну допомогу, евакуацію, медичні послуги, виплати та адміністративні сервіси. Водночас вони ж

стали й головною мішенню для зловмисників, які прагнули через кібератакки, інформаційні вкиди та дискредитаційні кампанії підірвати їхню репутацію та функціональність (Котух 2020: 567).

Саме тому питання кібербезпеки сьогодні напряму впливає не лише на технічну захищеність цифрових систем, а й на політичну стабільність, соціальну згуртованість і демократичну консолідацію українського суспільства. Високий рівень інформаційного захисту забезпечує безперервну комунікацію між владою та громадянами, формує довіру до демократичних процедур, захищає право громадян на доступ до правдивої інформації та знижує ефективність ворожих інформаційно-психологічних операцій. З іншого боку, слабкість у сфері кіберзахисту може призвести до дестабілізації регіону, політичної кризи та розбалансування державного управління в умовах війни. Тому Харківщина сьогодні є не лише об'єктом інформаційного впливу, а й важливим осередком практичного досвіду, який може бути використаний для удосконалення національної системи кібербезпеки.

На Харківщині, яка навіть в умовах тривалого воєнного стану продовжує забезпечувати стабільне функціонування місцевого самоврядування, обласної військової адміністрації, комунальних служб і громадських організацій, питання захисту інформаційного простору набуло стратегічного значення. Особлива увага приділяється захисту цифрових каналів комунікації, які в умовах обмежених фізичних контактів стали основним засобом взаємодії між владою та населенням, а також платформою для інформування про безпекову ситуацію, гуманітарну допомогу, адміністративні послуги та евакуаційні заходи. Оперативне реагування на інформаційні загрози стало необхідною умовою збереження суспільної довіри, адже у воєнний час поширення фейків, маніпулятивних повідомлень і неправдивих заяв може мати катастрофічні наслідки для громадського порядку, морального стану населення та легітимності влади (Бухарєв 2018).

Довіра громадян до демократичних процесів, зокрема до діяльності місцевих рад, військових адміністрацій, виборчих комісій та громадських ініціатив, значною мірою залежить від того, наскільки надійно захищено офіційні інформаційні ресурси, наскільки прозоро та відповідально організовано обробку та подання інформації, а також наскільки оперативно та ефективно спростовуються неправдиві повідомлення і дезінформаційні вкиди. Зниження рівня довіри внаслідок інформаційних атак може призвести до відмови людей виконувати розпорядження органів влади, участі в громадських заходах або до поширення панічних настроїв. Саме тому питання інформаційної безпеки сьогодні має не лише технічний, а й безпосередньо політичний і суспільний вимір.

В.В. Лизанчук справедливо зазначає, що інформаційна безпека неможлива без гармонізації національних і міжнародних підходів, а ефективність усіх заходів у цій сфері безпосередньо залежить від здатності адаптувати загальні принципи до конкретних локальних умов, політичного контексту, соціальної ситуації та реальних викликів безпеки, з якими стикається суспільство (Лизанчук 2017). Адже універсальні стандарти, розроблені в рамках міжнародних організацій, мають бути гнучко інтегровані у реалії кожного окремого регіону, щоб максимально ефективно відповідати на специфічні загрози і враховувати локальну інфраструктуру, рівень цифрової грамотності населення, характер інформаційного середовища і навіть соціально-політичні особливості регіону.

Харківщина яскраво підтверджує цю тезу своїм практичним досвідом, адже регіональне впровадження міжнародних стандартів і рекомендацій у сфері кібербезпеки не лише дозволяє підсилити захист інформаційних систем, а й формує нову демократичну культуру в цифровій площині. Завдяки цим процесам прозорість, підзвітність органів влади, доступність та безпека офіційної інформації поступово стали пріоритетами щоденної роботи як місцевої влади, так і громадських структур, волонтерських організацій та незалежних ЗМІ (Мотивація посадових осіб органів публічної влади 2012)

Проаналізований досвід Харківської області у сфері кібербезпеки наочно демонструє, що сучасна інформаційна безпека – це далеко не лише питання технічного захисту серверів, мережевих протоколів чи захищеності паролів. Насамперед це фундаментальна складова демократичної стабільності, суспільної згуртованості та політичної єдності. Інформаційна безпека гарантує без перерв-ний доступ громадян до об'єктивної, перевіреної інформації, формує довіру до легітимних державних і регіональних інституцій, забезпечує функціонування виборчих процесів, електронного врядування, систем оповіщення та надання

адміністративних послуг у воєнний і кризовий час.

Харківщина, як один із ключових регіонів на сході України, в умовах активних бойових дій і постійних інформаційних атак стала не лише об'єктом потужних кібератак і інформаційних спецоперацій, а й майданчиком для апробації ефективних моделей інформаційного захисту, організації спільного спротиву та розбудови систем кібербезпеки. Досвід Харківської області переконливо доводить, що кібербезпека повинна розглядатися як комплексний багаторівневий процес, у якому обов'язково поєднуються високотехнологічні рішення, організаційні механізми кризового реагування, міжнародна співпраця, регулярні освітні ініціативи та активна участь громадянського суспільства.

З одного боку, завдяки системному впровадженню рекомендацій Стратегії кібербезпеки України (Про рішення Ради національної безпеки і оборони України 2021), адаптації міжнародних стандартів і методик до місцевих умов, Харківщина змогла суттєво підвищити рівень технічної захищеності державних і комунальних інформаційних систем, захистити електронні ресурси обласної військової адміністрації, органів місцевого самоврядування, підприємств критичної інфраструктури, місцевих медіа та громадських організацій. Особливий акцент зроблено на захист виборчих процесів, безперебійну роботу електронного врядування, сервісів е-демократії та онлайн-доступу до адміністративних послуг у критичних умовах.

В умовах війни та постійної загрози поширення дезінформації особливо важливо забезпечити стабільну, оперативну та прозору комунікацію органів влади з населенням. Рекомендовано вдосконалити офіційні сайти обласних і районних адміністрацій, запровадити регулярні стріми, брифінги, відеозвернення, оперативні повідомлення в Telegram-каналах і соціальних мережах. Це дозволить мінімізувати вплив фейкових новин, оскільки перевірена інформація від офіційних джерел буде доступною швидко та без затримок. Доцільно розробити єдині стандарти кризової комунікації для місцевих органів влади, які регламентуватимуть порядок інформування населення у випадках надзвичайних ситуацій та інформаційних атак.

Доцільно організувати такі центри на базі профільних університетів, IT-кластерів або центрів підготовки фахівців у сфері кібербезпеки. Вони мають стати постійно діючими структурами, що координуватимуть роботу кіберволонтерів, IT-активістів, представників місцевих органів влади та бізнесу. Функції таких центрів мають включати моніторинг регіонального інформаційного простору, аналіз інформаційних загроз, оперативне реагування на кіберінциденти, організацію навчань і тренінгів, розробку локальних рекомендацій із захисту інформаційних ресурсів. Це дозволить сформувати єдиний центр компетенцій у регіонах та підвищити їхню стійкість до кіберзагроз.

Налагодження постійного діалогу, обмін досвідом та спільні навчання з міжнародними експертами у сфері кібербезпеки є критично важливими для підвищення як регіональної, так і національної безпеки. Варто розширювати партнерства з профільними структурами ЄС, НАТО, ОБСЄ, USAID, міжнародними IT-компаніями, дослідницькими центрами та українською діаспорою у сфері інформаційної безпеки. Це не лише зміцнить обороноздатність регіонів, а й дозволить Україні інтегруватися у світову систему колективної кібербезпеки.

СПИСОК ЛІТЕРАТУРИ

1. Дубов, Д. В. 2013. Стратегічні аспекти кібербезпеки України. *Стратегічні пріоритети* 4: 119–127.
2. Бухарєв, В. В. 2018. Адміністративно-правові засади забезпечення кібербезпеки України: автореф. дис... канд. юрид. наук: 12.00.07. Суми: Сумський державний університет.
3. Корнієнко, Б. Я. 2018. Безпека інформаційно-комунікаційних систем та мереж: навч. посіб. для студентів спец. 125 «Кібербезпека». Київ: НАУ.
4. Макаренко, Є. А. 2011. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст». *Актуальні проблеми міжнародних відносин* 102: 51–62 URL: http://apir.iir.edu.ua/index.php/apmv/article/view/2116/1879 .
5. Дзюндзюк, В. Б. 2018. Інформаційна війна як важлива складова сучасної гібридної війни. *Публічне управління XXI століття: світові практики та національні перспективи*: XVIII Міжнародний науковий конгрес «Публічне управління XXI століття: світові практики та національні перспективи». Харків: ХарРІ НАДУ: 169–172.
6. Котух, Є. В. 2020. Електронний уряд і кібербезпека у соціальних мережах: особливості реалізації. *Вісник НУЦЗ України*. Серія: Державне управління 2: 583-591. URL:

http://repositsc.nuczu.edu.ua/bitstream/123456789/18688/1/vdu13.pdf
7. Лизанчук, В. В. 2017. *Інформаційна безпека України: теорія і практика*: підручник. Львів: Видавничий центр Львівського національного університету ім. І. Франка.
8. Мотивація посадових осіб органів публічної влади при запровадженні сервісів е-урядування / В. В. Комаровський, В. А. Яценко, В. І. Бондарук, О. В. Нюнько, І. В. Комаровський. 2012. *Теоретичні та прикладні питання державотворення*. Вип. 10: 373-428. URL: file:///C:/Users/intel/Downloads/tppd_2012_10_27%20(1).pdf
9. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

Стаття надійшла до редакції 24.02.2025
Стаття рекомендована до друку 28.03.2025.

Oleksandra Zinchenko
PhD Student at the Department of Political Science of School of Philosophy
V.N. Karazin Kharkiv National University
alekca.98@ukr.net, https://orcid.org/0000-0003-1623-957X

CYBERSECURITY AS AN ELEMENT OF DEMOCRATIC CONSOLIDATION: LESSONS FROM KHARKIV REGION

In the context of hybrid warfare and targeted information aggression, the issue of cybersecurity is gaining particular importance not only as a technical challenge, but also as a key factor in ensuring national, political and social stability. Cybersecurity is emerging as an important element of democratic development, as information attacks are often aimed at undermining public trust, destabilising local governance and devaluing democratic institutions. The experience of Ukraine, namely the Kharkiv region, is considered as a significant example of how regional communities can withstand complex cyber and information challenges. The example of the Kharkiv region shows not only technical but also a clear political colouring of cyber threats, namely: massive DDoS attacks on public services, hacking of information resources, phishing campaigns, spyware, attacks on local media, active use of bot farms in social networks, i.e. everything that serves as a tool to pressure public opinion, create panic, discredit local governments and spread disinformation.

The article emphasises the particular danger of information campaigns that masquerade as legitimate sources but aim to spread hostile propaganda narratives, reduce the level of critical thinking and create an environment hostile to democratic values. These cyber tools can be aimed at both undermining the electoral process and creating artificial discontent among the population. At the same time, the example of the Kharkiv region demonstrates that with proper coordination between the authorities, law enforcement agencies, media and civil society, it is possible to effectively counter cyber threats. It is concluded that raising the level of digital literacy of the population, building local cyber defence systems, information transparency and engaging citizens in countering disinformation contribute to the formation of a sustainable democracy.

In such conditions, not only technical defenses but also the informational resilience of communities becomes a decisive factor in countering hybrid threats. This approach not only safeguards critical infrastructure but also strengthens public trust in democratic institutions.

Keywords: *cybersecurity, democratic consolidation, information operations, societal resilience, bot farms, regional security.*

REFERENCES

1. Dubov, D. 2013. Strategic aspects of Ukraine's cybersecurity. *Strategic priorities* 4: 119–127 (in Ukrainian).
2. Bukharev, V. V. 2018. *Administrative and Legal Principles for Ensuring Cybersecurity in Ukraine*: Author's Abstract. dis... Candidate of Legal Sciences: 12.00.07. Sumy: Sumy State University (in Ukrainian).

3. Kornienko, B. Security of Information and Communication Systems and Networks: a Textbook for Students of Speciality 125 «Cybersecurity». Kyiv: NAU. (in Ukrainian).
4. Makarenko, E. 2011. International Cooperation in the Sphere of Information Security: Regional Context. *Current Problems of International Relations.* URL: http://apir.iir.edu.ua/index.php/apmv/article/view/2116/1879 (in Ukrainian).
5. Dzyundzyuk, V. 2018. Information warfare as an important component of modern hybrid warfare. *Public administration of the 21st century: world practices and national perspectives*: XVIII International Scientific Congress «Public administration of the 21st century: world practices and national perspectives». Kharkiv: KharRI NAPU (in Ukrainian).
6. Kotukh, E. 2020. Electronic government and cybersecurity in social networks: implementation features. Bulletin of the National Center for Public Administration of Ukraine. Series: State Administration 583-591. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/18688/1/vdu13.pdf (in Ukrainian).
7. Lyzanchuk, V. 2017. *Information Security of Ukraine: Theory and Practice*: Textbook. Lviv: Publishing Center of the Ivan Franko National University of Lviv (in Ukrainian).
8. Motivation of public officials in the implementation of e-government services / V. V. Komarovsky, V. A. Yatsenko, V. I. Bondaruk, O. V. Nyunko, I. V. Komarovsky 2012. Theoretical and applied issues of state building. Issue 10: 373-428. URL: file:///C:/Users/intel/Downloads/tppd_2012_10_27%20(1).pdf (in Ukrainian).
9. On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 «On the Cybersecurity Strategy of Ukraine»: Decree of the President of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (in Ukrainian).

The article was received by the editors 24.02.2025 .
The article is recommended for printing 28.03.2025