

Наталія СТЕПАНЕНКО

Університет економіки та права “КРОК”,
доцент кафедри теорії та історії держави і права,
доктор філософії в галузі права, доцент,
м. Київ, вул. Табірна, 30–32, Україна, 03113
nataliasv@krok.edu.ua
ORCID: 0000-0001-6216-2206

ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ В УМОВАХ ЦИФРОВИХ ТЕХНОЛОГІЙ ПІД ЧАС ВОЄННОГО КОНФЛІКТУ

<http://doi.org/10.23939/law2025.46.312>

© Степаненко Н., 2025

В умовах повномасштабного збройного конфлікту, спричиненого агресією російської федерації проти України, цифрові технології стали невід’ємною частиною як бойових дій, так і повсякденного життя цивільного населення. Це створює безпрецедентні виклики для забезпечення та захисту прав людини. У статті проаналізовано ключові проблеми, що виникають на перетині цифрових технологій, прав людини та збройного конфлікту в українському контексті. Розглянуто використання цифрових платформ для поширення дезінформації та пропаганди, що порушує право на отримання достовірної інформації, а також заходи протидії цим явищам і пов’язані з ними ризики обмеження свободи слова. Проаналізовано загрози для права на приватність та захист персональних даних, зумовлені посиленням державного спостереження та збором даних в умовах воєнного стану, наголошено на важливості дотримання принципів законності та мінімізації даних. Висвітлено вплив кібератак на критичну інфраструктуру як на чинник порушення соціально-економічних прав цивільного населення та складності правової кваліфікації таких дій. Водночас показано позитивний потенціал цифрових технологій як інструменту для документування воєнних злочинів та порушень прав людини за допомогою даних з відкритих джерел (OSINT), фото- та відеофіксації, підкреслено важливість дотримання стандартів роботи з цифровими доказами (наприклад, Протоколу Берклі). Стаття базується на аналізі актуальних досліджень українських наукових установ, правозахисних та експертних організацій. Зроблено висновок про потребу комплексного підходу, що містить вдосконалення національного законодавства та міжнародно-правових норм, посилення кібербезпеки, розробку стандартів роботи з цифровими доказами і забезпечення балансу між потребами національної безпеки та захистом фундаментальних прав і свобод людини в умовах війни.

Ключові слова: права людини, цифрові технології, воєнний стан, збройний конфлікт, Україна, кібербезпека, дезінформація, захист персональних даних, цифрові докази.

Постановка проблеми. Сучасні збройні конфлікти дедалі більше характеризуються інтенсивним використанням цифрових технологій. Від систем озброєння і розвідки до комунікації та інформаційного впливу – цифрова сфера стала повноцінним театром воєнних дій. Повномасштабна агресія РФ проти України з лютого 2022 року яскраво продемонструвала цю тенденцію. Цифрові

інструменти активно використовують обидві сторони конфлікту, а також цивільне населення, що неминуче впливає на стан забезпечення прав людини. Виникають нові форми порушень, пов'язані з дезінформацією, кібератаками, цифровим спостереженням, водночас з'являються нові можливості для фіксації злочинів та захисту прав. Ця складна взаємодія потребує глибокого аналізу, особливо в контексті тривалого воєнного стану в Україні.

Аналіз останніх досліджень і публікацій. Питання впливу цифрових технологій на права людини в умовах конфлікту, кібербезпека в умовах воєнного стану, проблеми захисту персональних даних, питання використання цифрових доказів та міжнародних стандартів їх збору формують основу для розуміння багатогранності проблем, які активно досліджують такі українські фахівці: В. А. Бочковой, Н. А. Бааджи, Д. М. Белов, І. Є. Переш, І. Покорба, О. В. Петришин, О. С. Гиляка, К. В. Денисенко, І. С. Борко, О. М. Косов, О. О. Тихомиров, А. В. Шевчук, І. В. Гайдук та ін.

Нерозв'язані раніше частини загальної проблеми. Попри значну увагу до теми, низка аспектів залишається недостатньо вирішеною. По-перше, це адаптація норм міжнародного гуманітарного права до реалій кібервійни, зокрема чітка кваліфікація кібератак на цивільну інфраструктуру як воєнних злочинів. По-друге, брак уніфікованих та загальновизнаних стандартів верифікації і допустимості цифрових доказів, зібраних з відкритих джерел чи громадянами, у міжнародних судових інстанціях. По-третє, складність досягнення належного балансу між посиленням заходів безпеки та спостереження в умовах воєнного стану та захистом права на приватність і свободу вираження поглядів. По-четверте, питання транскордонного переслідування за кіберзлочини та поширення дезінформації, що здійснюються з території держави-агресора.

Формулювання мети. Метою статті є аналіз основних викликів та проблем у сфері забезпечення прав людини, пов'язаних із застосуванням цифрових технологій в умовах збройного конфлікту на території України, а також окреслення потенційних шляхів їх вирішення на основі аналізу актуальних вітчизняних досліджень, звітів експертних організацій та правових джерел.

Виклад основного матеріалу. Збройний конфлікт в Україні відбувається в епоху глибокої цифровізації суспільства, що породжує специфічні та багатогранні виклики для захисту прав людини, водночас відкриваючи нові можливості для їх утвердження та документування порушень.

Концепція “цифрових прав людини” виникла для вирішення унікальних викликів та можливостей, що постали в цифрову епоху. Ці права охоплюють традиційні права людини, оскільки вони застосовуються в онлайн-середовищі, а також нові права, специфічні для цифрової сфери, такі як право на доступ до інтернету, захист даних та цифрова ідентичність. В. А. Бочковой, Н. А. Бааджи вважають, що цифрові права людини – це сукупність прав і свобод, які захищають індивідуумів у цифровому середовищі, зокрема право на комунікацію, свободу контенту, цифрову ідентичність та набуття цифрових навичок [1, с. 229].

Погоджуємось з думкою науковців, які підкреслюють, що цифрові права людини стають невід'ємною частиною сучасного суспільства, де технології стрімко змінюють спосіб життя та взаємодії [2, с. 112].

О. В. Петришин, О. С. Гиляка зазначають, що ера цифрових технологій дає цілковито нові та якісно інші можливості для реалізації прав людини, але водночас створює нові виклики та загрози для їх забезпечення [3, с. 10].

Міжнародне право у сфері прав людини, зокрема Загальна декларація прав людини та Європейська конвенція з прав людини, слугує основою для захисту цифрових прав. Стаття 10 ЄКПЛ гарантує право на свободу вираження поглядів, яке поширюється на всіх без винятку, також користувачів онлайн-середовища [4].

Національне законодавство України, зокрема Конституція (стаття 34), Закон “Про інформацію” та Закон “Про захист персональних даних” також регулює аспекти цифрових прав [5]. Стаття 34 Конституції України гарантує кожному право на свободу думки і слова, вільне вираження своїх поглядів і переконань, а також право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або іншим способом. Право на приватність закріплено в міжнародних документах та конституціях більшої частини держав світу, також України.

У контексті дії правового режиму воєнного стану в Україні актуалізується проблема тимчасового обмеження фундаментальних прав людини, зокрема цифрових прав, з метою забезпечення національної безпеки. Проте, відповідно до міжнародно-правових стандартів у сфері прав людини, такі обмеження повинні мати легітимний характер, бути обґрунтованими нагальною суспільною потребою та пропорційними меті, яка ставиться. Обмеження інформаційних прав в умовах збройного конфлікту можуть бути зумовлені об’єктивною потребою збереження життєздатності нації, що корелює з правом держави вдаватися до заходів, які обмежують окремі права громадян задля гарантування безпеки та ефективності оборонних операцій.

Аналіз практики України свідчить про часткове відступлення від зобов’язань за статтею 10 Європейської конвенції з прав людини (ЕКПЛ) щодо свободи вираження поглядів та доступу до інформації у зв’язку з введенням воєнного стану.

Концепція цифрових прав перебуває на етапі динамічного розвитку, а її імплементація в умовах збройного конфлікту характеризується додатковою складністю. У цьому контексті особливо гостро постає питання забезпечення балансу між інтересами національної безпеки та правами особистості. Незважаючи на те, що основоположні принципи прав людини є універсальними та застосовуються в онлайн-середовищі, конкретні межі та допустимі обмеження цифрових прав залишаються предметом наукових дискусій та правового визначення.

Воєнний стан являє собою виняткову обставину, яка може слугувати підставою для відхилення від стандартів мирного часу. Однак такі відхилення потребують ретельного контролю з метою запобігання зловживанням та підтвердження їхньої дійсної потреби та пропорційності. Взаємодія між міжнародним правом прав людини та національним законодавством у сфері регулювання цифрових прав під час збройного конфлікту є визначальною. Національне законодавство повинно демонструвати узгодженість з міжнародними стандартами для забезпечення належного рівня захисту, одночасно враховуючи специфічні внутрішні потреби та виклики, що постають перед державою.

Правова база України у сфері цифрових прав формується під впливом як міжнародних конвенцій, так і власних конституційних та законодавчих положень. Аналіз послідовності та узгодженості різних рівнів правового регулювання є ключовим для розуміння загального ступеня захисту, що надається особам у цифровому просторі в умовах війни.

Використання цифрових технологій під час війни в Україні спричинило численні виклики для прав людини, зокрема кібератаки, спрямовані на критичну інфраструктуру та цивільних осіб [6]. Поширеними стали кампанії з дезінформації, спрямовані на маніпулювання громадською думкою та підриг довіри. Були висловлені занепокоєння щодо порушень приватності внаслідок витоків даних та стеження. Фейкова інформація поширювалася з 2014 року з метою дестабілізації України. Дезінформація спотворює громадську думку як в Україні, так і за її межами, вказує на те, що неправдива інформація може спричинити паніку та погіршити імідж керівництва, повідомляє про втручання російських хакерів в українське телерадіомовлення та атаки на вебсайти ЗМІ.

Українські науковці активно досліджують вплив цих цифрових загроз на права людини під час війни. У праці Л. І. Мазуренко розглядаються виклики та загрози інформаційній безпеці в умовах російсько-української війни, зокрема поширення дезінформації через соціальні мережі та важливість протидії неправдивій інформації [7, с. 45]. У статті А. І. Русакевича аналізується інформаційна безпека в

умовах воєнного стану в аспекті забезпечення інформаційних прав громадян, висвітлюються правові, політичні та технічні елементи цього питання. Досліджуються також правові аспекти забезпечення інформаційної безпеки під час повномасштабного вторгнення, наголошуючи на потребі захисту політичних прав і свобод в інформаційному просторі [8, с. 60].

Порушення права на публікацію контенту в цифрових медіа кваліфікується як порушення цифрових прав особистості та фундаментальних принципів свободи вираження поглядів, закріплених у статті 19 Загальної декларації прав людини [9, с. 92].

У контексті збройного конфлікту інформація набуває стратегічного значення, трансформуючись в інструмент впливу, а цифровий простір стає ключовою ареною протистояння. Це зумовлює потребу комплексного підходу, що становить забезпечення кібербезпеки як технічного аспекту захисту інформаційних систем, так і інформаційно-психологічної безпеки, спрямованої на протидію деструктивним інформаційним впливам та маніпуляціям.

Результати наукових досліджень підтверджують, що сучасний збройний конфлікт має не лише кінетичний, але й виражений інформаційний вимір. Цифрові платформи значно розширюють географію охоплення та інтенсивність поширення як верифікованої, так і недостовірної інформації, що актуалізує проблему розуміння впливу інформаційних потоків на дотримання прав людини, психологічний стан індивідів та національну безпеку держави.

Систематичне акцентування на загрозах дезінформації та кібератак у досліджуваних матеріалах свідчить про наявність цілеспрямованих та скоординованих зусиль, спрямованих на дестабілізацію України за допомогою використання цифрових інструментів. Це має безпосередній вплив на широкий спектр прав людини, зокрема право на отримання об'єктивної та достовірної інформації, свободу вираження поглядів (яка може обмежуватися через цензурування альтернативних думок або маніпулювання інформаційним простором) і право на приватність (що порушується внаслідок несанкціонованого доступу до персональних даних).

Консистентність виявлених загроз у різних інформаційних джерелах та впродовж тривалого часу вказує на стратегічний характер дій агресора. Аналіз тактичних прийомів, стратегічних цілей та оперативного впливу цих цифрових операцій є критично важливим для розробки ефективних контрзаходів та забезпечення захисту прав людини в цифровому середовищі.

Дослідження, проведені українськими науковцями, наголошують на потребі застосування багатоаспектного підходу до розв'язання зазначених проблем, що містить не лише впровадження правових та технічних механізмів, але й реалізацію заходів, спрямованих на підвищення рівня медіаграмотності та формування навичок критичного мислення серед населення. Протидія дезінформації та мінімізація наслідків кібератак потребують від суспільства формування стійкості до маніпулятивних впливів та підвищення обізнаності щодо потенційних ризиків у цифровому просторі. Освітні та інформаційні кампанії відіграють ключову роль у розширенні можливостей громадян щодо захисту власних прав та зміцнення національної інформаційної безпеки.

Обмежений доступ до інтернету в зонах бойових дій та на окупованих територіях становить значний виклик для прав людини, перешкоджаючи доступу до інформації, комунікації та основних послуг [10, с. 63]. Повідомлялося про цензуру та блокування онлайн-ресурсів, особливо тих, що сприймаються як проросійські. Є занепокоєння щодо незаконного стеження та потенційного зловживання персональними даними, зібраними через цифрові платформи [11]. Поширення ворожої пропаганди та дезінформації залишається серйозною проблемою, впливаючи на громадську думку та потенційно підбурюючи до насильства [12, с. 291]. Росія навмисно від'єднала доступ до інтернету на окупованих територіях, що збігалось з порушеннями прав людини. У цій праці мовиться про експерта, який виступає проти серйозних обмежень інтернету під час війни,

наголошуючи на потребі збереження свободи вираження поглядів. Він зазначає, що від'єднання та збої в роботі мережі завдають шкоди бізнесу, екстреним службам, журналістам та право-захисникам.

Українські науковці задокументували конкретні виклики та їх наслідки для прав людини, зокрема обмеження інтернету в Україні під час війни, згадуючи занепокоєння щодо блокування урядом проросійських ресурсів та регулювання ІТ-сектору; порушення цифрових та інформаційних прав внаслідок кібератак та дезінформації; зазначається, що право на доступ до інформації може бути обмежене в умовах воєнного стану в Україні з міркувань національної безпеки.

Навмисне націлювання на інтернет-інфраструктуру та запровадження від'єднань на окупованих територіях свідчить про стратегію контролю інформаційних потоків та ізоляції населення, що потенційно сприяє порушенням прав людини та перешкоджає підзвітності. Обмежуючи доступ до зовнішнього світу та перешкоджаючи спілкуванню всередині окупованих територій, окупаційні сили сприяють ізоляції населення, що створює атмосферу безкарності. Це ускладнює для жертв можливість повідомляти про зловживання, а для міжнародних спостерігачів – збір об'єктивної інформації та моніторинг порушень прав людини. Пошук правильного балансу є вирішальним для уникнення підриву демократичних цінностей в ім'я безпеки. Надмірно широкі або непрозорі обмеження доступу до інтернету та контенту можуть мати непередбачені наслідки, такі як придушення законного інакомислення, перешкоджання роботі журналістів та правозахисників, а також створення можливостей для поширення неперевіраних чуток та дезінформації. Вразливість персональних даних в умовах війни є значним занепокоєнням, оскільки витоки даних можуть піддати осіб підвищеному ризику заподіяння шкоди, особливо тих, хто був переміщений або постраждав від конфлікту. Електронні реєстри, що містять конфіденційну інформацію про ВПО, жертв війни та отримувачів соціальної допомоги, є потенційними цілями для кібератак. Компрометація цих даних може призвести до крадіжки особистих даних, шахрайства, дискримінації або навіть фізичної шкоди.

Хоча Україна має міцну основу, законодавство потребує вдосконалення з урахуванням міжнародних стандартів, виникає потреба узгодження цифрових практик з міжнародними стандартами прав людини та забезпечення кібербезпеки. Український уряд активно використовував цифрові технології для підтримки управління, надання послуг та спілкування зі своїми громадянами під час війни, демонструючи значний рівень цифрової стійкості. Швидке впровадження та розширення таких платформ, як "Дія", для надання основних послуг, у поєднанні із зусиллями щодо забезпечення інтернет-з'єднання, незважаючи на пошкодження інфраструктури, підкреслюють стратегічну важливість цифрової трансформації в умовах кризи. Залучення міжнародних партнерів, зокрема технологічні компанії та інші уряди, було вирішальним у підтримці цифрової інфраструктури та зусиль України у сфері кібербезпеки. Це підкреслює транснаціональний характер цифрової безпеки та важливість міжнародної співпраці у вирішенні воєнних викликів у цифровій сфері.

Надання таких послуг, як Starlink, передання конфіденційних даних за кордон для захисту та обмін досвідом та ресурсами демонструють колективні зусилля, спрямовані на зміцнення цифрової оборони України та підтримку основних онлайн-функцій. Українські експерти визнають потребу постійного вдосконалення правової бази та практичних заходів для захисту цифрових прав під час війни. Це охоплює адаптацію законодавства до конкретних викликів збройного конфлікту, зміцнення можливостей кібербезпеки та сприяння цифровій грамотності серед населення. Динамічний характер як цифрових технологій, так і самого конфлікту зумовлює потребу постійної оцінки та вдосконалення стратегій захисту прав людини в цифровій сфері. Це потребує прихильності до навчання на власному досвіді та адаптації до нових загроз та викликів.

Право на свободу вираження поглядів стикається з викликами через цензуру, обмеження певного контенту та криміналізацію висловлювань, що вважаються такими, що підривають національну безпеку. Доступ до інформації ускладнюється пошкодженням інфраструктури, урядо-

ними обмеженнями щодо певних даних з міркувань безпеки та цифровою нерівністю. Приватність перебуває під загрозою через стеження, витoki даних та потенційне зловживання персональною інформацією, зібраною онлайн. Безпека даних є надзвичайно важливою через ризик кібератак, спрямованих на конфіденційну інформацію та критичну інфраструктуру

Українські науковці наголошують на важливості узгодження національних законів з міжнародними принципами прав людини в цифровій сфері, виступають за посилення міжнародної правової бази для врегулювання цифрових прав під час збройних конфліктів, визнаючи, що національного законодавства може бути недостатньо для боротьби з транснаціональними загрозами та забезпечення підзвітності. Заклик до нової міжнародної конвенції про цифрові та інформаційні права людини відображає усвідомлення того, що чинне міжнародне право може недостатньо враховувати специфічні виклики, пов'язані з цифровими технологіями в контексті збройного конфлікту. Це підкреслює потребу більш комплексного та адаптованого підходу на глобальному рівні. Акцент на узгодженні українського законодавства зі стандартами ЄС відображає ширші прагнення країни до європейської інтеграції та визнання розвиненої правової бази ЄС у таких сферах, як захист даних та кібербезпека. Прийняття норм ЄС може допомогти Україні зміцнити захист цифрових прав та сприяти більшій сумісності та співпраці з європейськими партнерами у боротьбі з цифровими загрозами. Дослідження підкреслює динамічний характер цифрового середовища та потребу постійної адаптації правових норм та механізмів правозастосування для того, щоб йти в ногу з технологічним прогресом та еволюцією загроз. Швидкий розвиток цифрових технологій, таких як штучний інтелект та дипфейки, створює нові виклики для захисту прав людини. Правові рамки повинні бути гнучкими та адаптованими для ефективного розв'язання цих нових проблем.

Водночас, попри всі виклики, цифрові технології стали потужним інструментом для захисту прав людини та документування звірств агресора. Можливості фіксації подій за допомогою смартфонів та інших мобільних пристроїв, аналіз супутникових знімків високої роздільної здатності, а також збір та верифікація даних з відкритих джерел (OSINT – Open Source Intelligence) дають змогу документувати воєнні злочини, злочини проти людяності та інші грубі порушення прав людини у безпрецедентних раніше масштабах [13]. Ці цифрові докази мають потенціал стати ключовими у розслідуваннях та судових процесах як на національному рівні, так і в міжнародних інстанціях (Міжнародний Кримінальний Суд, Міжнародний Суд ООН). Однак для забезпечення юридичної сили та допустимості таких доказів їх збір, збереження, аналіз та представлення суду вимагають дотримання суворих міжнародно визнаних процедур та стандартів, таких як, наприклад, Протокол Берклі щодо використання цифрової інформації з відкритих джерел у розслідуваннях [14].

Отже, цифровізація глибоко і подвійно впливає на ситуацію з правами людини в умовах збройного конфлікту в Україні, створюючи як серйозні загрози, так і унікальні можливості.

Висновки. Дослідження свідчить про неоднозначний вплив цифрових технологій на забезпечення прав людини в умовах збройного конфлікту в Україні. З одного боку, процеси цифровізації супроводжуються виникненням нових ризиків та викликів, зокрема, у сфері інформаційної війни, розширення практик цифрового спостереження та зростання уразливості до кібератак. З другого – цифрові технології відкривають безпрецедентні можливості для ефективного документування міжнародних злочинів, мобілізації суспільства та розширення доступу громадян до інформації.

Ефективне реагування на ці протиріччя потребує комплексного, системного підходу, що передбачає постійне вдосконалення національної нормативно-правової бази та гармонізацію міжнародних норм для їх адаптації до цифрових реалій сучасного збройного конфлікту. Зокрема, треба посилити технічні, організаційні та правові заходи щодо забезпечення кібербезпеки об'єктів критичної інфраструктури та захисту персональних даних, а також розробити та імплементувати уніфіковані стандарти збору, фіксації, збереження та використання цифрових доказів у судочинстві.

Особлива увага має бути надана підвищенню рівня цифрової компетентності та медіа-грамотності населення як превентивному механізму протидії деструктивним інформаційно-психологічним впливам та дезінформаційним кампаніям. Загалом пошук та підтримка оптимального балансу між легітимними заходами державної безпеки в умовах воєнного стану та гарантуванням непорушності фундаментальних прав і свобод людини є визначальним завданням для подальших наукових досліджень у цьому напрямі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бочковой В. А., Бааджи Н. А. (2024). Цифрові права людини та їх обмеження в умовах сучасних правових викликів. *Науковий вісник Ужгородського Національного Університету*. С. 228–233.
2. Белов Д. М., Переш І. Є., Покорба І. (2024). Цифрові права людини: доктринальні засади. *Електронне наукове видання “Аналітично-порівняльне правознавство”*. С. 110–115.
3. Петришин О. В., Гиляка О. С. (2021). Права людини у цифрову епоху : виклики, загрози та перспективи. *Вісник Національної академії правових наук України*. Т. 28. № 1. С. 7–35.
4. Свобода слова в Інтернеті. ГО “Платформа прав людини”. Міжнародні та національні стандарти свободи слова в Інтернеті. URL: <https://ppl.org.ua/bibliotech/mizhnarodni-ta-nacionalni-standarti-svobodi-slova-v-interneti> (Дата звернення: 30.03.2025).
5. Законодавство про захист даних в Україні. URL: <https://www.dlapiperdataprotection.com/index.html?t=law&c=UA> (Дата звернення: 30.03.2025).
6. Що вони робили в тіні: відключення інтернету та звірства в Україні. URL: <https://www.accessnow.org/internet-shutdowns-and-atrocities-in-ukraine> (дата звернення: 30.03.2025).
7. Мазуренко Л. І. (2022). Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна*. Серія “Питання політології”, Випуск 42. С. 50. URL: <https://doi.org/10.26565/2220-8089-2022-42-08> (Дата звернення: 30.03.2025).
8. Русакевич А. (2024). Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав громадян. *Law. State. Technology*. Вип. 2. С. 58–62.
9. Денисенко К. В., Борко І. С., Косов О. М. (2023). Реалізація цифрових та інформаційних прав людини в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету*, Серія ПРАВО. Вип. 77: част. 1. С. 90–94.
10. Тихомиров О. О. (2022). Проблеми обмеження інформаційних прав людини в умовах воєнного стану в Україні. *Juris Europensis Scientia*. Вип. 6. С. 62–67.
11. Інтернет в умовах війни: чи необхідні обмеження в Україні. URL: <https://vgoru.org/prava-lyudini/internet-v-umovakh-viiny-chy-neobkhidni-obmezhenia-v-ukraini> (Дата звернення: 30.03.2025).
12. Вплив дезінформації на національну безпеку України в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2024. № 2. С. 290–292. URL: http://lsej.org.ua/2_2024/71.pdf (Дата звернення: 30.03.2025).
13. Війна у цифровому вимірі та права людини : підсумковий звіт. Платформа прав людини. Київ, 2023. 38 с. URL: https://ppl.org.ua/wp-content/uploads/2023/11/vijna-u-cifrovomu-vimiri-ta-prava-lyudini_pidsumkovij-zvit.pdf (Дата звернення: 30.03.2025).
14. Документування воєнних злочинів: як працює протокол Берклі? / Експертний Центр з Прав Людини. 02.02.2023. URL: <https://ecpl.com.ua/news/dokumentuvannia-voiennykh-zlochyniv-iak-pratsiuie-protokol-berkli/> (Дата звернення: 30.03.2025).
15. Шевчук А. В., Гайдук І. В. (2022). Захист персональних даних в умовах воєнного стану в Україні. *Право і безпека*. № 2 (85). С. 103–110. URL: <https://pb.univd.edu.ua/index.php/PB/article/download/722/585/> (Дата звернення: 30.03.2025).

REFERENCES

1. Bochkova, V. A., Baadzhi, N. A. (2024). *Digital Human Rights and Their Limitations in the Context of Modern Legal Challenges* // Scientific Bulletin of Uzhhorod National University. P. 228–233. [In Ukrainian].
2. Belov, D. M., Peresh, I. Ye., Pokorba, I. (2024). *Digital Human Rights: Doctrinal Foundations* // Analytical and Comparative Jurisprudence. P. 110–115. [In Ukrainian].

3. Petryshyn, O. V., Hilyaka, O. S. (2021). **Human Rights in the Digital Age: Challenges, Threats, and Prospects** // Bulletin of the National Academy of Legal Sciences of Ukraine. Vol. 28. No. 1. P. 7–35. [In Ukrainian].
4. **Freedom of Speech on the Internet. Human Rights Platform NGO. International and National Standards of Freedom of Speech on the Internet**. Retrieved from: <https://ppl.org.ua/bibliotech/mizhnarodni-ta-nacionalni-standarti-svobodi-slova-v-interneti> (Accessed: 30.03.2025). [In Ukrainian].
5. Data Protection Legislation in Ukraine. Retrieved from: <https://www.dlapiperdataprotection.com/index.html?t=law&c=UA> (Accessed: 30.03.2025). [In Ukrainian].
6. **What They Did in the Shadows: Internet Shutdowns and Atrocities in Ukraine**. Retrieved from: <https://www.accessnow.org/internet-shutdowns-and-atrocities-in-ukraine> (Accessed: 30.03.2025). [In Ukrainian].
7. Mazurenko, L. I. (2022). **Information Security in the Context of the Russian-Ukrainian War: Challenges and Threats** // Bulletin of V. N. Karazin Kharkiv National University. Series: Political Science Issues. Iss. 42. P. 50. DOI: <https://doi.org/10.26565/2220-8089-2022-42-08> (Accessed: 30.03.2025) [In Ukrainian].
8. Rusakevych A. (2024). **Information Security in the Conditions of Martial Law in the Aspect of Ensuring Citizens' Information Rights** // Law. State. Technology. Issue 2. P. 58–62. [In Ukrainian].
9. Denysenko, K. V., Borko, I. S., Kosov, O. M. (2023). **Implementation of Digital and Information Human Rights in the Conditions of Martial Law** // Scientific Bulletin of Uzhhorod National University. Law Series. Iss. 77, Part 1. P. 90–94. [In Ukrainian].
10. Tikhomirov, O. O. (2022) **Problems of Restricting Information Rights in the Conditions of Martial Law in Ukraine** // Juris Europensis Scientia. Issue 6. P. 62–67. [In Ukrainian].
11. **Internet in Wartime: Are Restrictions Necessary in Ukraine?** Retrieved from: <https://vgoru.org/prava-lyudini/internet-v-umovakh-viiny-chy-neobkhidni-obmezhenia-v-ukraini> (Accessed: 30.03.2025). [In Ukrainian].
12. **The Impact of Disinformation on Ukraine's National Security Under Martial Law** // Legal Scientific Electronic Journal. 2024. No. 2. P. 290–292. Retrieved from: http://lsej.org.ua/2_2024/71.pdf (Accessed: 30.03.2025). [In Ukrainian].
13. **War in the Digital Dimension and Human Rights: Final Report**. Human Rights Platform. Kyiv, 2023. 38 p. Retrieved from: https://ppl.org.ua/wp-content/uploads/2023/11/vijna-u-czifrovomu-vimiri-ta-prava-lyudini_pidsumkovij-zvit.pdf (Accessed: 30.03.2025). [In Ukrainian].
14. **Documenting War Crimes: How Does the Berkeley Protocol Work?** / Expert Center for Human Rights. 02.02.2023. Retrieved from: <https://ecpl.com.ua/news/dokumentuvannia-voiennykh-zlochyniv-iak-pratsiuie-protokol-berkli/> (Accessed: 30.03.2025). [In Ukrainian].
15. Shevchuk, A. V., Haiduk, I. V. (2022). **Protection of Personal Data in the Conditions of Martial Law in Ukraine** // Law and Security. No. 2 (85). P. 103–110. Retrieved from: <https://pb.univd.edu.ua/index.php/PB/article/download/722/585/> (Accessed: 30.03.2025). [In Ukrainian].

Дата надходження статті: 18.02.2025 р.

Natalia STEPANENKO

PhD in law, associate Professor of the Department
of Theory and History of the State and Law of “KROK” University
Kyiv, 30–32, Tabirna str., Ukraine, 03113
nataliasv@krok.edu.ua
ORCID: 0000-0001-6216-2206

ENSURING HUMAN RIGHTS IN THE CONTEXT OF DIGITAL TECHNOLOGIES DURING AN ARMED CONFLICT

In the context of the full-scale armed conflict caused by the Russian Federation's aggression against Ukraine, digital technologies have become an integral part of both hostilities and the daily lives of the civilian population. This poses unprecedented challenges for ensuring and protecting human rights. The article analyzes the key issues arising at the intersection of digital technologies, human rights, and armed conflict in the Ukrainian context. It examines the use of digital platforms for

spreading disinformation and propaganda, which violates the right to receive reliable information, as well as countermeasures against these phenomena and the associated risks of restricting freedom of speech. Threats to the right to privacy and personal data protection, stemming from increased state surveillance and data collection under martial law, are analyzed, emphasizing the importance of adhering to the principles of legality and data minimization. The impact of cyberattacks on critical infrastructure as a factor violating the socio-economic rights of the civilian population and the complexity of legally qualifying such actions are highlighted. Simultaneously, the positive potential of digital technologies as a tool for documenting war crimes and human rights violations using open-source intelligence (OSINT), photo, and video evidence is demonstrated, underscoring the importance of adhering to standards for handling digital evidence (e.g., the Berkeley Protocol). The article is based on the analysis of current research by Ukrainian academic institutions, human rights, and expert organizations. It concludes that a comprehensive approach is necessary, including improving national legislation and international legal norms, strengthening cybersecurity, developing standards for working with digital evidence, and ensuring a balance between national security needs and the protection of fundamental human rights and freedoms in wartime.

Keywords: human rights, digital technologies, martial law, armed conflict, Ukraine, cybersecurity, disinformation, personal data protection, digital evidence.