

УДК 342.7:005.25:(351.9-052:004)

DOI 10.32755/sjlaw.2024.01.

Денисенко К. В.,

кандидат наук з державного управління, доцент, доцент кафедри адміністративного, цивільного та господарського права і процесу юридичного факультету, Пенітенціарна академія України, м. Чернігів, Україна
ORCID: 0000-0002-9637-1361;

Борко І. С.,

курсантка 147 навчальної групи, Пенітенціарна академія України, м. Чернігів, Україна
ORCID: 0000-0002-3397-0121;

Дегтяр Д. С.,

студент 148 навчальної групи, Пенітенціарна академія України, м. Чернігів, Україна
ORCID: 0009-0002-5331-2713

ПЕРСПЕКТИВИ ЗАПРОВАДЖЕННЯ ІНСТИТУТУ ЦИФРОВОГО ОМБУДСМЕНА ЯК МЕХАНІЗМУ ЕФЕКТИВНОЇ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНИХ ТА ЦИФРОВИХ ПРАВ ЛЮДИНИ

Стаття присвячена формуванню пропозицій щодо запровадження інституту цифрового омбудсмена як механізму ефективної реалізації інформаційних і цифрових прав людини. Сформовано авторське бачення поняття цифрових та інформаційних прав людини як взаємопов'язаних і взаємозалежних категорій прав людини, що визначають її діяльність у цифровому та інформаційному середовищах і передбачають низку супутніх прав у будь-якій сфері її життєдіяльності.

Ключові слова: інформаційна безпека, інформація, інформаційне середовище, інформаційні права людини, цифрові права людини, цифрові технології, діджиталізація.

Постановка проблеми. Процес цифровізації в Україні виходить на суцільно новий рівень. У сучасному глобалізованому світі важко уявити людину, яка не користується смартфоном, комп'ютером або мережею Інтернет. Стрімкий розвиток цифрових технологій сприяє діджиталізації суспільства, формуванню світу «без кордонів», де кожен може отримати майже будь-яку інформацію, а також розвитку цифрових та інформаційних прав людини.

Поряд з цим в умовах сучасності на практиці мають місце численні випадки порушення інформаційних та цифрових прав людини. У зв'язку з цим виникає необхідність удосконалення інституційного механізму забезпечення цифрових і інформаційних прав людини для безпечного її існування в цифровому та інформаційному середовищах.

Аналіз останніх досліджень і публікацій. Серед вітчизняних учених, наукові дослідження яких становлять основу пізнання теоретико-практичних засад реалізації цифрових та інформаційних прав людини, є: О. Б. Братасюк, А. В. Марущак, Н. Ф. Ментух, Н. І. Ткачук, М. Г. Хаустова та ін. Водночас питання щодо вдосконалення інституційного забезпечення реалізації інформаційних та цифрових прав людини потребують додаткової уваги з огляду на численні випадки їх порушення.

Метою статті є формування пропозицій щодо запровадження інституту цифрового омбудсмена як механізму ефективної реалізації інформаційних та цифрових прав людини.

Виклад основного матеріалу. Цифрові та інформаційні права взаємозалежні та взаємопов'язані категорії, оскільки існування цифрового світу базується на наявності інформації, а пошук інформації залежить від наявності доступу до носія інформації (в сьогоденних реаліях зазвичай це комп'ютер та мережа Інтернет). Розглядаючи безпосередньо таку категорію прав людини як цифрові права, ми повинні звернути увагу, що на сьогодні законодавчо закріплене визначення «цифрові права людини» відсутнє, але існує низка різних доктринальних визначень.

Так, одні науковці вважають, що цифрові права – це права людини, які полягають у праві людей на доступ, використання, створення та публікацію цифрових творів, доступ і використання комп'ютерів та інших електронних пристроїв, а також комунікаційних мереж, зокрема, до мережі Інтернет [1]. Інші ж вказують, що цифрові права людини – це окрема група прав людини, які пов'язані з використанням та/або реалізуються в мережі Інтернет за допомогою спеціальних пристроїв (комп'ютерів, смартфонів тощо) [2, с. 59]. Аналізуючи вищевказане, доцільно підкреслити, що необхідними елементами цифрових прав людини є електронні пристрої та мережа Інтер-

нет. Уся діяльність людини, що здійснюється з їх використанням, гарантує окремі права людини, що об'єднані в таку категорію як «цифрові права».

Науковці до цифрових прав відносять: право на доступ до інтернету; свобода вираження поглядів онлайн; право на приватність і захист персональних даних; право на свободу та особисту безпеку онлайн; право на мирні зібрання, асоціації та/або використання електронних інструментів демократії; право на цифрове самовизначення, або право від'єднуватися від онлайн, або бути забутим в онлайні [2, с. 59].

Загальні права людини, що закріплені в різних нормативно-правових документах, інтегруються в «цифру» і надають певні гарантії сучасній людині. Наприклад, право на доступ до інтернету можна розцінювати як право на інформацію, гарантоване статтею 34 Конституції України. Право на мирні зібрання також закріплені Конституцією України статтею 39. Свобода вираження поглядів онлайн приховує в собі положення статті 10 Європейської Конвенції про захист прав людини і основоположних свобод. І так можна навести приклади до всіх цифрових прав, які виділені науковцями, що дає нам можливість дійти висновку – цифрові права є певною інтеграцією сукупності прав людини в сучасний цифровий формат її життєдіяльності.

Необхідно зазначити той факт, що одні дослідники зараховують цифрові права в окрему категорію, що охоплює специфіку реалізації та гарантії захисту фундаментальних прав людини в інтернеті, зокрема свободи вираження поглядів і права на приватність онлайн. Інші акцентують увагу на похідності цифрових прав від інформаційних, однак не ототожнюють їх [3, с. 193]. Погляди наукової спільноти щодо дефініції інформаційних прав людини переважно доповнюють одна одну і переплітаються між собою, оскільки сама назва вже говорить сама за себе.

Ткачук Н. І. зазначає, що інформаційні права і свободи людини й громадянина – це гарантовані державою можливості особи задовольняти свої потреби в отриманні, використанні, поширенні, охороні і захисті необхідного для життєдіяльності обсягу інформації, комунікаційні права, право на безпечне інформаційне середовище тощо [4, с. 28]. Деякі науковці

об'єднують інформаційні права із комунікаційними і пропонують п'ять напрямків їх розвитку, а саме у вигляді права на доступ і доступність, право на критичну компетентність, право на діалог і право на приватність [5, с. 58].

Інформаційні права людини – це гарантовані державою у сфері інформаційного середовища можливості особи, що містять у собі низку прав: право на створення, поширення, зберігання, отримання інформації; право на використання інформації; право на свободу думки і слова; право на комунікацію; право на безпечне інформаційне середовище; право на рівний доступ до інформації; право на обрання способу поширення інформації; право на захист конфіденційної інформації. Таким чином, ми можемо прослідкувати взаємовідношення між цифровими та інформаційними правами, що дозволяє нам об'єднати їх в єдине ціле і вивести власне авторське визначення: *цифрові та інформаційні права людини* – це взаємопов'язані та взаємозалежні категорії прав людини, що визначають її діяльність у цифровому та інформаційному середовищах та передбачають низку супутніх прав у будь-якій сфері її життєдіяльності.

До 24 лютого 2022 р. було здійснено низку заходів для розвитку цифрового та інформаційного суспільства. Нагальними питаннями були і залишаються – підвищення рівня безпеки українців у цифровому та інформаційному середовищах, а також поєднання реалізації цифрових та інформаційних прав людини. Під останнім доцільно розуміти належний захист та легкий доступ власника до особистих документів за допомогою мобільного пристрою. У контексті цього визначним стало ухвалення розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку електронного урядування в Україні» від 20 вересня 2017 року № 649-р. Цей документ став правовою основою для розвитку діяльності органів публічного адміністрування у цифровому та інформаційному середовищах.

У 2019 році Міністерство цифрової трансформації України оголосило про створення сайту «Дія» та анонсувало бетаверсію однойменного мобільного застосунку. Характерним є те, що для українців користування «Дією» виявилось дуже простим. На початку люди звісно не розуміли що до чого, але з ча-

сом прийшло розуміння і станом на 23 серпня 2022 року вже 18 мільйонів користувачів є у застосунку «Дія» [6]. Однак із самого початку створення «Дії» було багато скептицизму. Почалося все з промови Володимира Зеленського у травні 2019 року. Він озвучив ідею «держава в смартфоні» [7]. Після такої промови Президента України було створено Міністерство цифрової трансформації України на чолі з Михайлом Федоровим, який керував розробкою онлайн-сервісу «Дія». Ідея цього мобільного застосунку полягала в тому, щоб українці могли не носити всі документи із собою, а мати просто телефон із встановленим застосунком «Дія» і за необхідності користуватися інформацією, що міститься в цьому мобільному застосунку.

Значна частина українців почала використовувати «Дію» після карантину у зв'язку із поширенням гострої респіраторної хвороби Covid-19. Наявність документів, що посвідчують особу, та поява сертифікатів про вакцинацію сприяли популярності «Дії». Згодом розробники почали додавати різні функції, що допомогло сервісу здобути довіру українців. Станом на кінець 2021 року на порталі «Дія» вже було доступно 72 послуги, а в застосунку – 9 послуг та 15 цифрових документів [8].

Не менш важливим кроком для реалізації цифрових та інформаційних прав людини в Україні було ухвалення Закону України «Про внесення змін до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» від 30 березня 2021 року № 1368-IX. Було введено нові поняття як «Е-паспорт» та «Е-паспорт для виїзду за кордон», а також внесено зміни до статті 14¹, згідно з якими Е-паспорт і е-паспорт для виїзду за кордон формуються за бажанням особи, на ім'я якої оформлено паспорт громадянина України у формі картки або паспорт громадянина України для виїзду за кордон, оформлені із застосуванням засобів Реєстру, та використовуються на території України для посвідчення особи та підтвердження громадянства, надання адміністративних та інших послуг, крім випадків, передбачених частиною третьою цієї статті. Е-паспорт і е-паспорт для виїзду за кордон пред'являються особою замість та без додаткового

пред'явлення паспорта громадянина України, паспорта громадянина України для виїзду за кордон, документів (відомостей, даних) про реєстраційний номер облікової картки платника податків, про місце проживання [9]. Доцільним вважаємо наголосити на значущості забезпечення права на захист конфіденційної інформації, що потребує посиленого захисту. У цьому випадку одразу виступає реалізація цифрових прав людини, які допоможуть у захисті інформації. У 21 столітті багато інформації зберігається на електронних носіях, тому першочерговим є створення засад захисту цих носіїв. Найпростішим прикладом буде вже згадана нами «Дія», де для того, щоб увійти в систему, необхідно пройти аутентифікацію. Як один з можливих варіантів, через систему BankID.

Система BankID Національного банку – це державна система віддаленої ідентифікації, яка забезпечує передачу персональних даних користувачів від банку, в якому відкрито рахунок, до суб'єкта, який надає користувачу послугу [10]. Також особа може використовувати цю технологію, щоб самостійно зберігати та захищати особисту інформацію (фотографії, документи, музику тощо). Мінімальним, але часто важливим елементом захисту, є пароль. Він може бути різним, але найкращим вважається той, що має малі та великі літери, цифри та спеціальні символи. Також доцільно запам'ятовувати пароль, а не записувати його. Якщо людина зберігає велику кількість інформації на різних сервісах, носіях тощо, то важливо до кожного носія створити новий пароль, що не буде повторюватися. Однак постає питання: як всі ці паролі запам'ятати? Відповідь дуже проста і полягає в тому, що не треба запам'ятовувати всі паролі, достатньо запам'ятати один, який буде ключем до всіх паролів. Всі ці паролі необхідно зберігати у спеціальних програмах, що і будуть тримати їх у своїй пам'яті. До таких програм можна віднести Last pass, One password та інші. Усі вони діють за одним принципом – знати пароль до такої програми.

У контексті реалізації права на захист конфіденційної інформації доцільно розглянути Закон України «Про захист персональних даних». В умовах сучасності кожна людина реалізовує окреслене право, наприклад, реєструючись на сайті та «ставля-

чи галочку» на згоду обробки персональних даних. Відповідно до вищезгаданого Закону персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована; обробка персональних даних – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем [11]. З вищевказаного випливає, що персональні дані – це інформація про фізичну особу. Тобто, погоджуючись на обробку персональних даних, особа надає згоду на певні дії з такою інформацією. І це є певним ризиком розповсюдження особистої інформації.

У багатьох випадках у користувачів взагалі не має вибору: особа змушена передати свої дані, бо в іншому разі вона взагалі не зможе користуватись тим чи іншим сервісом. Така згода є умовно добровільною [12, с. 125].

Після повномасштабного вторгнення російської федерації на територію України розпочалася війна як на воєнному фронті, так і на кібер- та інформаційному просторах. У результаті цього реалізація цифрових і інформаційних прав людини постійно перебуває у зоні ризику. Російська федерація поширює фейкові новини, здійснює примусове під'єднання українських громадян до власної мережі Інтернет із блокування інформації, що таким чи іншим чином пов'язана з Україною, вдається до хакерських атак цивільного населення, державних сайтів та медіаресурсів України. Серед таких атак доцільно виокремити деякі, що були здійснені з початку повномасштабного вторгнення:

– *хакерські атаки на сайти органів державної влади в Україні*. 23 лютого 2022 року відбулася атака на державні сайти. Не працювали портали Кабінету Міністрів України, Верховної Ради України, Міністерства закордонних справ. Також з труднощами працював сайт Служби безпеки України [13];

– *розсилання електронних листів «від імені органів державної влади України» цивільним громадянам*. 26.07.2022 року урядова команда реагування на комп'ютерні надзвичайні

події України CERT-UA, яка діє при Держспецзв'язку, повідомила про масове розповсюдження небезпечних електронних листів з темами «Інформаційний бюлетень» та «Бойове розпорядження». Вони надходять на приватні адреси e-mail, зокрема, начебто від Національної академії Служби безпеки України [14];

– **здійснення шахраями дзвінків цивільним громадянам.** Генеральний штаб попередив про шахраїв, що телефонують родичам військовослужбовців Збройних сил, які потрапили в полон або вважаються безвісти зниклими. «Користуючись емоційним станом рідних і близьких, зловмисники телефонують з прихованих номерів та пропонують за грошову винагороду «надати інформацію» про військового й «сприяти визволенню з полону». Також шахраї намагаються, нібито щоб уточнити, дізнатися особисті дані українських захисників», – заявив Генштаб [15];

– **поширення фейкової інформації через взламвання засобів масової інформації України та/або через соціальні мережі.** 21.07.2022 року здійснено кібератаку на сервери та мережі радіостанцій TAVR Media. В управлінні радіогрупи – дев'ять провідних радіостанцій: Хіт FM, Radio ROKS, KISS FM, Radio RELAX, Мелодія FM, Наше Радіо, Radio JAZZ, Classic Radio і віднедавна – Радіо Байрактар. Кіберзловмисники розповсюдили інформацію про те, що Президент України Володимир Зеленський нібито перебуває в реанімації, а його обов'язки виконує голова Верховної Ради Руслан Стефанчук [16];

– **розсилання файлів із вірусами через електронну пошту та месенджери.** 02.06.2022 року урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA попередила про нові небезпечні електронні листи з файлом «зміни оплати праці з нарахуваннями.docx», які отримували працівники державних організацій України. Відкриття документа загрожує ураженням комп'ютера шкідливою програмою Cobalt Strike Beacon [17];

– **блокування доступу до українських інформаційних ресурсів та від'єднання українських операторів зв'язку на окупованих територіях.** 30.05.2022 року українські оператори мобільного зв'язку, інтернет-послуг та телефонії почали фіксувати спочатку перебої, а потім і повне від'єднання зв'язку

в Херсонській області. Відповідно до отриманої від компаній інформації відбулося втручання представників окупаційного режиму в роботу обладнання – від'єднання живлення обладнання, кабелів тощо. Це вже не перша спроба позбавити українських громадян, які опинилися на тимчасово окупованих територіях, можливості зв'язатися з рідними, викликати швидко допомогу чи рятувальників, отримати правдиву інформацію про перебіг війни та ситуацію в країні [18].

З метою з'ясування думки громадян щодо стану забезпечення їхніх цифрових та інформаційних прав людини авторами дослідження протягом жовтня–листопада 2023 року було проведено опитування через платформу Google Forms на тему «Сучасний стан забезпечення цифрових та інформаційних прав людини» (<https://forms.gle/T93Xwt5HAcLpASjo7>), де взяло участь 227 осіб. Усього було 9 питань, що містили відкриту відповідь і варіанти. Серед респондентів: 83,9 % (190 осіб) – жінки, 16,1 % (37 осіб) – чоловіки. Крім цього, 67,7 % (153 особи) – особи віком від 18–35 років, 16,1 % (37 осіб) – до 18 років і 16,1 % (37 осіб) – старше 35 років.

Учасникам опитування було запропоновано обрати, які твердження вони вважають порушенням цифрових та інформаційних прав людини, однак, одне твердження було хибним. Отже, поява спаму під час перегляду фільму обрали 35,5 % (81 особа) респондентів; заборона соціальних мереж чи сайтів новин – 67,7 % (154 особи); поширення Вашої конфіденційної інформації – 100 % (227 осіб); поширення спотвореної або неправдивої інформації – 87,1 % (198 осіб); відмова державного службовця розповісти інформацію, що є службовою – 22,6 % (51 особа).

Далі пропонувалось оцінити за шкалою від 0–5 стан забезпечення цифрових та інформаційних прав людини в Україні до початку війни і 48,4 % (110 осіб) опитуваних оцінили цей стан на 3 бали; 25,8 % – на 4 бали (58 осіб); 16,1 % (37 осіб) – 2 бали, 6,5 % (15 осіб) – на 5 балів; 3,2 % (7 осіб) – на 1 бал і 0 % (0 осіб) на 0 балів. Найбільше оцінки обґрунтовувалися наявністю таких проблем, як: поширення спаму як через інтернет-зв'язок так і через телефонний; продаж конфіденційної інформації користувачів; наявність фейкових новин та вірусів;

низька цифрова грамотність населення і відсутність механізму захисту цифрових та інформаційних прав людини.

Наступне питання полягало в необхідності оцінити рівень захисту цифрових та інформаційних прав людини в Україні в умовах воєнного стану. 38,7 % (88 осіб) опитуваних оцінюють рівень на 3 бали; 22,6 % – на 4 бали (51 особа); 22,6 % – на 2 бали (51 особа); 6,5 % – на 5 балів (15 осіб); 6,5 % – на 1 бал (15 осіб); 3,2 % – на 0 балів (7 осіб). Серед проблем, які наявні сьогодні в Україні, учасники дослідження назвали: наявність неправдивої інформації; масові кібератаки російських хакерів.

71 % (161 особа) опитуваних вважають, що заходи захисту цифрових та інформаційних прав людини в наш час є достатніми, 29 % (66 осіб) мають протилежну думку. 100 % (227 осіб) респондентів згодні з тим, що в Україні необхідно вдосконалювати систему нормативно-правового регулювання та адміністративні заходи забезпечення цифрових та інформаційних прав людини. 90,3 % (204 особи) підтримали пропозицію запровадження цифрового омбудсмена, 9,7 % (23 особи) – не вважають це доцільним.

Таким чином, сучасний стан забезпечення цифрових та інформаційних прав людини характеризується наявністю низки порушень зазначених прав і серйозною загрозою функціонування безпечного цифрового та інформаційного середовища. У результаті опитування було виявлено, що більшість респондентів все ж таки вважають заходи захисту цифрових та інформаційних прав людини в умовах воєнного стану достатніми, при цьому усі респонденти погодилися, що існує потреба в удосконаленні нормативно-правової бази та адміністративних заходів забезпечення цифрових і інформаційних прав людини. 90,3 % (204 особи) опитуваних також підтримали пропозицію запровадження посади цифрового омбудсмена.

Україна є однією з держав, що прогресують у цифровій сфері, але на основі вищевикладених результатів дослідження ми можемо зробити висновок, що наявна на сьогодні організаційно-правова система забезпечення цифрових та інформаційних прав людини потребує вдосконалення.

Відповідно до статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» суб'єктами в цій галузі є: Президент України через Раду національної безпеки і оборони України; Національний координаційний центр кібербезпеки; Кабінет Міністрів України; міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності тощо [19]. В умовах воєнного стану діяльність зазначених вище суб'єктів спрямована на викриття злочинів проти основ національної безпеки України, опосередковано торкаючись питання захисту цифрових та інформаційних прав людини. Проаналізувавши законодавство, ми можемо дійти висновку, що в Україні відсутній парламентський контроль у сфері захисту цифрових та інформаційних прав людини. Хоча при Верховній Раді України і діють окремі комітети з питань цифрової трансформації та з питань гуманітарної і інформаційної політики, до повноважень яких входять контрольні функції, все ж цього виявляється недостатньо.

Для усунення вказаних недоліків ми пропонуємо запровадити інститут цифрового омбудсмена. Цю ідею підтримали більшість респондентів проведеного авторами опитування. Важливість його запровадження полягає в тому, що він буде здійснювати контроль за забезпеченням цифрових та інформаційних прав людини та допомагати вищеназаним суб'єктам кібербезпеки України вдосконалювати свою діяльність.

До повноважень цифрового омбудсмена будуть входити: 1) прийом звернень від громадян щодо порушень їхніх цифрових та інформаційних прав людини; 2) направлення звернень громадян до уповноважених органів (за необхідності); 3) здійснення щорічних доповідей про факти порушень цифрових та інформаційних прав людини, а також результати усунення вказаних недоліків; 4) підвищення рівня цифрової та інформаційної грамотності населення; 5) організація заходів правопросвіти населення України у сфері цифрових та інформаційних прав людини; 6) контроль, координація та розроблення рекомендацій удосконалення діяльності суб'єктів забезпечення циф-

рової та інформаційної безпеки України; 7) сприяння приведенню законодавства України у сфері цифрових та інформаційних прав людини відповідно до міжнародних стандартів; 8) розвиток міжнародного співробітництва у сфері цифрових та інформаційних прав людини.

Діяльність цифрового омбудсмена повинна ґрунтуватися на таких принципах: верховенства права; законності; гуманізму; поваги до прав людини; співпраці у сфері захисту цифрових та інформаційних прав людини; відкритості та прозорості; доброчесності та етичної поведінки; інноваційності та відкритості до змін.

Для більш ефективної роботи цифрового омбудсмена пропонуємо також розробити мобільний застосунок, в якому доцільно розробити такі опції: можливість подання звернень до цифрового омбудсмена (за допомогою аутентифікації через застосунок «Дія»); доступ до нормативно-правових актів України у сфері захисту цифрових та інформаційних прав людини, а також міжнародно-правових актів; можливість фіксації порушень цифрових та інформаційних прав людини; інформація про діяльність цифрового омбудсмена, щорічні доповіді; інформація про механізми захисту інформаційних та цифрових прав людини; навчальні матеріали у сфері цифрової та інформаційної грамотності для різної вікової категорії.

Для реалізації вищезазначеного доцільними є розроблення та ухвалення Закону України «Про Уповноваженого Верховної Ради України з цифрових та інформаційних прав людини» для закріплення посади цифрового омбудсмена на законодавчому рівні, а також співпраця Міністерства цифрової трансформації України з Уповноваженим Верховної Ради України з цифрових та інформаційних прав людини і Верховною Радою України щодо створення мобільного застосунку.

Висновки. Таким чином, проведене дослідження продемонструвало численні випадки порушень інформаційних та цифрових прав людини. Особливого загострення зазначене набуло в умовах повномасштабного вторгнення російської федерації на територію України. Проведене авторами анкетування щодо стану забезпечення їхніх цифрових та інформаційних прав людини продемонструвало необхідність запровадження інституту

цифрового омбудсмена. Цю ідею підтримали більшість респондентів проведеного авторами опитування. Важливість його запровадження полягає в тому, що він буде здійснювати контроль за забезпеченням цифрових та інформаційних прав людини і допомагати суб'єктам забезпечення кібербезпеки вдосконалювати свою діяльність.

Список використаних джерел

1. Цифрові права українців або Декларація цифрових прав людини : вебсайт. URL: <https://www.businesslaw.org.ua/digital-rights-t/> (дата звернення: 24.12.2023).

2. Братасюк О. Б., Ментух Н. Ф. Поняття та класифікація цифрових прав в Україні. *Юридичний науковий електронний журнал*. 2021. № 10. С. 58–61.

3. Мединська О. Я., Синоруб Г. П. Права людини та цифрова трансформація. *Людина в українському суспільстві в системі цінностей прав людини: сучасний вимір медіадіяльності* : матеріали Всеукраїнської науково-практичної конференції (м. Київ, 14 травня 2021 р.). Київ, 2021. С. 192–196.

4. Ткачук Н. І. Інформаційні права і свободи людини і громадянина в Україні: визначення термінів, співвідношення понять. *Інформація і право*. 2018. № 2 (25). С. 17–30.

5. Hannu Nieminen Inequality, social trust and the media: Towards citizens' communication and information rights: web-site Digitala Vetenskapliga Arkivet. URL: <https://www.divaportal.org/smash/record.jsf?pid=diva2%3A1535715&dsid=-3490> (дата звернення: 24.12.2023).

6. У «Дії» вже 18 мільйонів користувачів – Мінцифри : вебсайт мультимедійної платформи іномовлення України «Укрінформ». URL: <https://www.ukrinform.ua/rubric-technology/3556364-u-dii-vze-18-miljoniv-koristuvaciv-mincifri.html> (дата звернення: 24.12.2023).

7. Я мрію про державу в смартфоні – Володимир Зеленський : вебсайт офіційного інтернет-представництва Президента України. URL: <https://www.president.gov.ua/news/ya-mriyu-pro-derzhavu-u-smartfoni-volodimir-zelenskij-55585> (дата звернення: 24.12.2023).

8. Цифрові паспорти, Covid-сертифікати, еПідтримка: 100 перемог Дії та Мінцифри : вебсайт державного онлайн-сервісу «Дія». URL: <https://diia.gov.ua/news/cifrovi-pasporti-sovid-sertifikati-yepidtrimka-100-peremog-diyi-ta-mincifri> (дата звернення: 24.12.2023).

9. Про внесення змін до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» : Закон України

від 30.03.2021 р. № 1368-IX. URL: <https://zakon.rada.gov.ua/laws/show/1368-20#Text> (дата звернення: 24.12.2023).

10. BankID НБУ : вебсайт Національного банку України. URL: <https://bank.gov.ua/ua/bank-id-nbu> (дата звернення: 24.12.2023).

11. Про захист персональних даних : Закон України від 01.06.2010 № 2297-XI. Дата оновлення: 19.08.2022. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#n11> (дата звернення: 24.12.2023).

12. Моргун А. М. Права людини і громадянина в інформаційній сфері. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання* : матеріали Всеукр. наук.-практ. конф. (м. Київ, 2 грудня 2021 р.). Київ – Одеса, 2021. С. 123–127.

13. Чергова кібератака: в Україні не працює низка держсайтів : вебсайт аналітичного порталу Слово і діло. URL: <https://www.slovoidilo.ua/2022/02/23/novyna/suspilstvo/cherhova-kiberataka-ukrayini-ne-pracuyue-nyzka-derzhajsitiv> (дата звернення: 24.12.2023).

14. Російські хакери знову атакують через електронні листи : вебсайт Державної служби спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/rosiiski-khakeri-znovu-atakuyut-cherez-elektronni-listi> (дата звернення: 24.12.2023).

15. Генштаб: Шахраї телефонують родичам полонених і пропонують «допомогти» з обміном за гроші : вебсайт Бабель. URL: <https://babel.ua/news/79011-genshtab-shahraji-dzvonyat-rodicham-polonenih-i-proponuyut-dopomogti-z-obminom-za-groshi> (дата звернення: 24.12.2023).

16. Хакери атакували українські радіостанції та розповсюдили фейк про проблеми зі здоров'ям Президента України : вебсайт Державної служби спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/khakeri-atakuvali-ukrayinski-radiostanciyi-ta-rozprovsyudili-feik-pro-problemi-zi-zdorov-yam-prezidenta-ukrayini> (дата звернення: 24.12.2023).

17. Увага! Нова кібератака на державні організації України, хакери використовують тему зарплат : вебсайт Державної служби спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-na-derzhavni-organizaciyi-ukrayini-khakeri-vikoristovuyut-temu-zarplat> (дата звернення: 24.12.2023).

18. Російські окупанти відключили зв'язок на півдні України : вебсайт Державної служби спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/rosiiski-okupanti-vidklyuchili-zv-yazok-na-pivdni-ukrayini> (дата звернення: 24.12.2023).

19. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#n62> (дата звернення: 24.12.2023).

Denysenko K.,

Ph.D. in Public Administration, Associate Professor,
Associate Professor of the Department of Administrative,
Civil and Commercial Law and Process of the Law Faculty,
Penitentiary Academy of Ukraine, Chernihiv, Ukraine
ORCID: 0000-0002-9637-1361;

Borko I.,

Cadet of the 147th academic group,
Penitentiary Academy of Ukraine, Chernihiv, Ukraine
ORCID: 0000-0002-3397-0121;

Dehtiar D.,

Student of the 148th academic group,
Penitentiary Academy of Ukraine, Chernihiv, Ukraine
ORCID: 0009-0002-5331-2713

PERSPECTIVES OF ESTABLISHMENT OF DIGITAL OMBUDSMAN'S INSTITUTION AS A MECHANISM FOR EFFECTIVE REALIZATION OF HUMAN INFORMATION AND DIGITAL RIGHTS

The article is devoted to the formation of propositions about establishing a digital ombudsman's institution as a mechanism for effective realization of human information and digital rights. It is emphasized that many cases of violations of human information and digital rights are in practice in modern conditions. In this regard it is necessary to improve the institution mechanism of human information and digital rights providing for safely human's being in digital and information environments.

Author vision of human digital and information rights as interrelated and interdependent human rights categories which define human activity in digital and information environments and provide for several related human rights in any sphere of activity is formed, propositions about establishment of the digital ombudsman's institution are also proved. This idea was supported by many respondents conducted by an author's poll.

Digital ombudsman's powers will be included: 1) accepting applications from citizens about human digital and information rights violations; 2) sending citizen's applications to authorized bodies (if necessary); 3) writing year's reports about facts human digital and information rights violations and results of elimination of indicated disadvantages; 4) increasing level of digital and information citizen's knowledge; 5) organization events of legal education for Ukrainian citizens in spheres of digital and information rights; 6) control, coordination and development recommendations of improvement activity of subjects who provide digital and information security of Ukraine; 7) making nationality law base in spheres of digital and information rights according to international standards; 8) developing international cooperation in spheres of human digital and information rights.

Key words: information security, information, information environment, human information rights, human digital rights, digital technologies, digitalization.

References

1. Digital rights of Ukrainians or Human digital rights Declaration : web-site, available at: <https://www.businesslaw.org.ua/digital-rights-t/> (accessed 24 December 2023).
2. Bratasiuk, O. B., Mentukh, N. F. (2021), "The concept and classification of digital rights in Ukraine", *Juridical scientific and electronic journal*, № 10, pp. 58–61.
3. Medynska, O. Ya., Synorub, H. P. (2021), "Human rights and digital transformation", *A human in Ukrainian society in human rights values` system: modern dimension of media`s work*: Ukrainian scientific-practical conference Kyiv, 14 May 2021, pp. 192–196.
4. Tkachuk, N. I. (2018), "Information rights and freedoms of human and citizen in Ukraine: definition of terms, relation of concepts", *Information and law*, № 2 (25), pp. 17–30.
5. Hannu Nieminen Inequality, social trust and the media: Towards citizens' communication and information rights: web-site Digitala Vetenskapliga Arkivet, available at: <https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1535715&dswid=-3490> (accessed 24 December 2023).
6. Diya has 18 million users – Mintsyfyry : web-site of National News Agency of Ukraine – "Ukrinform", available at: <https://www.ukrinform.ua/rubric-technology/3556364-u-dii-vze-18-miljoniv-koristuvaciv-mincifri.html> (accessed 24 December 2023).
7. I dream about a state in a smartphone – Volodymyr Zelensky: official web-site of the President of Ukraine, available at: <https://www.president.gov.ua/news/ya-mriyu-pro-derzhavu-u-smartfoni-volodimir-zelenskij-55585> (accessed 24 December 2023).
8. Digital passports, COVID-certificates, E-support: 100 Diya's victories and Mintsyfyry: web-site of state online-service "Diya", available at: <https://diia.gov.ua/news/cifrovi-pasporti-sovid-sertifikati-yepidtrimka-100-peremog-diyi-ta-mincifri> (accessed 24 Decemder 2023).
9. Ukraine (2021), On Amendments to the Law of Ukraine "On the Unified State Demographic Register and Documents Confirming Citizenship of Ukraine, Identity or Special Status", Kyiv.
10. BankID NBU : web-site of National bank of Ukraine, available at: <https://bank.gov.ua/ua/bank-id-nbu> (accessed 24 December 2023).
11. Ukraine (2010), On Personal Data Protection, Kyiv.
12. Morhun, A. M. (2021), "Human and citizen`s rights in information sphere", *Social and digital transformation: theoretical and practical*

problems of legal regulation : Ukrainian scientific-practical conference, 2 December 2021, Kyiv, Odesa, pp. 123–127.

13. Another cyber attack: a number of state sites do not work in Ukraine : web-site of the Analytical portal "Slovo i dilo", available at: <https://www.slovoidilo.ua/2022/02/23/novyna/suspilstvo/cherhova-kiberataka-ukrayini-ne-pracyuye-nyzka-derzhajtiv> (accessed 24 December 2023).

14. Russian hackers are attacking through emails again : web-site of State Service of Special Communications and Information Protection of Ukraine, available at: <https://cip.gov.ua/ua/news/rosiiski-khakeri-znovu-atakuvut-cherez-elektronni-listi> (accessed 24 December 2023).

15. General Staff: fraudsters call relatives of prisoners and offer to “help” in exchange for money : web-site Babel, available at: <https://babel.ua/news/79011-genshtab-shahraji-dzvonyat-rodicham-polonenih-i-proponuyut-dopomogti-z-obminom-za-groshi> (accessed 24 December 2023).

16. Hackers attacked Ukrainian radio stations and spread a fake about the health problems of the President of Ukraine : web-site of State Service of Special Communications and Information Protection of Ukraine, available at: <https://cip.gov.ua/ua/news/khakeri-atakuvali-ukrayinski-radiostanciyi-ta-rozpovsyudili-feik-pro-problemi-zi-zdorov-yam-prezidenta-ukrayini> (accessed 24 December 2023).

17. WARNING! New cyberattack on Ukrainian public organizations, hackers use the topic of salaries : web-site of State Service of Special Communications and Information Protection of Ukraine, available at: <https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-na-derzhavni-organizaciyi-ukrayini-khakeri-vikoristovuyut-temu-zarplat> (accessed 24 December 2023).

18. Russian Invaders Disabled Communication Services in the South of Ukraine : web-site of State Service of Special Communications and Information Protection of Ukraine, available at: <https://cip.gov.ua/ua/news/rosiiski-okupanti-vidklyuchili-zv-yazok-na-pivdni-ukrayini> (accessed 24 December 2023).

19. Ukraine (2017), On the Basic Principles of Cybersecurity in Ukraine, Kyiv.