УДК 004.056 *DOI: https://doi.org/10.32631/vca.2025.1.44*

Олександр Сергійович ПЕРЕДЕРІЙ,
кандидат юридичних наук, доцент
(Харківський національний університет імені В. Н. Каразіна, м. Харків)

Людмила Вікторівна КУЛАЧОК-ТІТОВА,
кандидат юридичних наук, доцент
(Харківський національний університет імені В. Н. Каразіна, м. Харків)

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЦИФРОВИХ ПОСЛУГ В АСПЕКТІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

У статті, застосовуючи методи комплексного аналізу, наводиться система організаційно-правових заходів забезпечення безпеки цифрових послуг в аспекті протидії кіберзлочинності в Україні. Зокрема, це зміцнення довіри приватного сектору та громадян до цифрових послуг, які надаються державою, безумовного виконання вимог щодо забезпечення кібербезпеки та кіберзахисту під час їх надання, розвиток національної інформаційної інфраструктури, розроблення національних стандартів у сфері кібербезпеки, створення органів з оцінки відповідності надавачів електронних довірчих послуг вимогам для кваліфікованих надавачів кваліфікованих електронних довірчих послуг та автентифікація їх користувачів, підвищення ефективності системи захисту персональних даних громадян шляхом гармонізації законодавства України з відповідним законодавством Європейського Союзу.

На основі аналізу положень актів чинного законодавства, які регламентують державну політику у сфері кібербезпеки, а також опрацювання аналітичних матеріалів із цих питань, розкрито зміст заходів

забезпечення цифрових послуг, а також акцентовано увагу на існуючий проблематиці їх повноцінної реалізації. Зокрема, це проблематика забезпечення безпеки користувачів найбільш державних електронних застосунків, збереження галузевого принципу інформатизації державних органів, оптимізація архітектоніки управління інформаційною безпекою, яку організації та органи державної влади можуть створювати, і використовувати для власного захисту, функціональні проблеми діяльності органів з оцінки відповідності надавачів електронних довірчих послуг встановленим вимогам, досягнення уніфікації процесу застосування методів автентифікації для всіх міністерств і відомств, проблематика здобуття налагодження ефективної співпраці європейськими партнерами на ринку цифрових послуг.

Обґрунтовано позицію про необхідність подальшої роботи з правової регламентації процедур досягнення безпечності і прозорості надання цифрових послуг, вчасне виявлення і нейтралізацію відповідних ризиків і загроз кібербезпеці. Відповідно, актуальним завданням юридичної науки є формування науково обґрунтованих пропозицій щодо удосконалення правового забезпечення розвитку як самого ринку цифрових послуг, так і убезпечення національного цифрового середовища.

Ключові слова: *Україна, кібербезпека, кіберзлочинність, цифрові послуги, інформаційна інфраструктура, законодавство, Європейський Союз, правові інновації, протидія кіберзлочинності.*

Постановка проблеми. Для сучасної України питання забезпечення кібербезпеки набуло особливої актуальності. В умовах протидії повномасштабному військовому вторгненню, усі елементи сектору безпеки і оборони України, а також структури цивільного народного господарства та громадянського суспільства докладають максимальних зусиль для убезпечення національного інформаційного простору від цілеспрямованих шкідливих впливів та інших форм кіберзлочинності. У зазначеному аспекті важливим є питання щодо забезпечення процесу формування, надання і споживання особливо важливого для соціуму різновиду послуг, які є цифровими. У відповідності до Закону України «Про цифровий контент та цифрові послуги» від 10.08.2023 р. № 3321-IX цифровими є послуги, що надають можливість споживачу створювати, обробляти, зберігати та поширювати дані у цифровій формі або отримувати доступ до таких даних, а також здійснювати будь-які інші дії з даними у цифровій формі, що були створені чи завантажені споживачем або іншими користувачами такої послуги (хостинг файлів, обробка текстів або ігри, які пропонуються в середовищі хмарних обчислень і соціальних мережах)[1]. Беручи до уваги різноманітність і популярність цифрових послуг, в останній час нормативно-правове регулювання забезпечення їх безпеки значно

[1] Про цифровий контент та цифрові послуги : Закон України від 10.08.2023 р. № 3321-IX. *Відомості Верховної Ради України*. 2023. № 90. Ст. 345

оновилося та удосконалилося.

Відповідно, актуальним науково-практичним завданням для вітчизняної юридичної науки є наукова розвідка організаційно-правових заходів забезпечення безпеки цифрових послуг як частини державної політики у сфері протидії кіберзлочинності.

Питання щодо організаційно-правових засад забезпечення цифрових послуг в Україні потрапляло у центр уваги вітчизняних правників у межах аналізу суміжної проблематики. Проте, наукова розробка захисту цифрових послуг в аспекті забезпечення кібербезпеки України є незначною. Інформаційним базисом для сформульованих у статті ідей і позицій стали положення нормативних актів про кібербезпеку, а також окремі наукові і експертні позиції М. Кінаша, А. Чорноус, М. Федорова.

Метою дослідження є висвітлення організаційно-правових заходів забезпечення безпеки цифрових послуг як складової кібербезпеки України.

Виклад основного матеріалу. Підіймаючи питання про надання цифрових послуг в Україні, слід відзначити, що врегулювання зазначеного інституту на рівні законодавства було вимогою Європейського Союзу. Так, юридичне інституціювання цифрових послуг стало наслідком сприйняття національною правовою системою України Директиви Європейського Парламенту і Ради (ЄС) № 2019/770 щодо певних аспектів, що стосуються контрактів на постачання цифрового контенту та цифрових послуг від 20.05.2019 р.[1]

Зауважимо, що з початку 2024 р. для забезпечення надання цифрової послуги належної якості, мають бути дотриманими два критерії, яким вона має відповідати: суб'єктивний та об'єктивний. Перший стосується умов, обумовлених споживачем і виконавцем у договорі, а другий виходить за межі домовленостей сторін і належить до питань придатності цифрової послуги встановленим стандартам і мети, для якої зазвичай використовують такі послуги. Також на нормативному рівні тепер чітко визначено права виконавця на модифікацію цифрової послуги, що надається безперервно та встановлено відповідальність виконавця цифрової послуги за їхню невідповідність визначеним критеріям. Зазначене, безперечно, урегульовує ринкові відносини у сфері цифрових послуг, обсяг і капіталізація яких невпинно зростає і має стійку тенденцію до збільшення.

Очевидним є те, що цифрові послуги як дороговартісний і складний технологічний інформаційний продукт може бути під загрозою неправомірного посягання, що, у свою чергу, тягне за собою комплексні ризики для системи кібербезпеки України. Задля недопущення цього, чинна Стратегія кібербезпеки України від 14.05.2021 р. передбачає систему організаційно-правових заходів забезпечення безпеки цифрових послуг[2]. У

[1] Цифрові послуги в Україні : особливості регулювання сфери: повідомлення від 22.02.2024 р. *Інтернет-сайт «Ligazakon»*. URL: https://biz.ligazakon.net/analitycs/225808_tsifrov-poslugi-v-ukran-osoblivost-regulyuvannya-sferi (дата звернення: 01.04.2025).

[2] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. *Офіційний вісник України*. 2021. № 70. Ст. 4417.

зазначеному документі визначено, що безпечні цифрові послуги досягаються шляхом забезпечення державою балансу між потребами суспільства, вітчизняного ринку, економіки держави та необхідними заходами з кібербезпеки, а також надійністю та безпекою цифрових послуг протягом усього їхнього життєвого циклу. Вказане є однією з умов досягнення стану кіберстійкості держави.

Аналіз положень Стратегії кібербезпеки України від 14.05.2021 р. дає підстави виокремити декілька базових організаційно-правових заходів убезпечення цифрових послуг від загроз. Зокрема, це

1) зміцнення довіри приватного сектору та громадян до цифрових послуг, які надаються державою, безумовного виконання вимог щодо забезпечення кібербезпеки та кіберзахисту під час їх надання та інформування громадськості про їх безпечність та надійність. Зауважимо, що впродовж останніх п'яти років держава досягла певних позитивних результатів у справі довіри громадян до цифрових послуг. Так, Міністерство цифрового багато цифрових послуг для громадян і українського бізнесу. Зокрема, Україна стала першою країною у світі, в якій цифровий паспорт має таку ж силу, що й паперовий чи пластиковий аналог. У застосунку «Дія» українці використовують 4,7 млн ID-карток, 12,2 млн закордонних паспортів та 6,6 млн водійських посвідчень, а серед найпополярніших послуг для підприємців – реєстрація ФОП та ТОВ на порталі Дія, що є найшвидшою реєстрацією бізнесу у світі[1]. Держава активно працює в напрямі забезпечення безпеки користувачів Дії (кілька разів було проведено програму Bug Bounty, в якій етичні хакери тестували застосунок і за винагороду в 1 млн. гривень шукали вразливості, але не знайшли).

2) впровадження цифрових послуг для населення та розвитку національної інформаційної інфраструктури. Ключовим, системоутворюючим елементом національної інформаційної інфраструктури є створення інформаційного ресурсу і формування оптимального правового режиму його використання. Базові кроки у цьому напрямі було зроблено. Проте, найбільш серйозною проблемою зазначеного напряму діяльності є галузевий принцип інформатизації державних органів, який досі зберігається. Як зауважує А. Чорноус, це є наслідком неузгодженості і несумісності форматів даних, які зберігаються в публічних інформаційних системах, відсутності сталої системи зберігання та архівування електронних баз даних органів публічної адміністрації, недосконалості нормативно-правової регламентації отримання доступу до інформаційних ресурсів публічної адміністрації[2]. Наразі триває робота з усунення зазначених чинників і впровадження у національну правову систему інноваційних правових інститутів.

[1] Михайло Федоров. Дії 3 роки. Як Україна отримала місце у світовій історії цифровізації? 14 лютого 2023. Економічна правда. URL: https://epravda.com.ua/columns/2023/02/14/697034/ (дата звернення: 28.03.2025).

[2] Чорноус А. Г. Інформаційні ресурси як елемент національної інформаційної інфраструктури: їх створення та використання. *Інформація і право*. 2018. № 3. С. 54

3) розроблення національних стандартів у сфері кібербезпеки, організаційних та технічних вимог, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів. Зазначений захід є комплексним, і відповідає інтересам розвитку цифрового бізнесу. Цифрові послуги передбачають торгівлю інформацією як товаром, а отже їх захист неможливий без запровадження управління інформаційною безпекою на основі стандартів інформаційної безпеки, яких існує значна кількість. Найбільш прийнятними серед них є ISO/IEC 2700 (міжнародний стандарт визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS),

Cybersecurity Framework NIST (забезпечує гнучкий підхід до управління ризиками, пов'язаними з кібербезпекою), PCI DSS (стандарт безпеки даних індустрії платіжних карток розроблений для забезпечення того, щоб компанії, які обробляють, зберігають або передають інформацію про кредитні картки, підтримували безпечне середовище)[1]. Зазначені стандарти не є вичерпними. На їх основі формується архітектоніка управління інформаційною безпекою, яку організації та органи державної влади можуть створювати, і використовувати для власного захисту.

4) створення органів з оцінки відповідності надавачів електронних довірчих послуг вимогам для кваліфікованих надавачів кваліфікованих електронних довірчих послуг. Головним органом є Кабінет міністрів України, який визначає організаційно-правовий порядок здійснення відповідної діяльності. Постановою Кабінету Міністрів України від 13 вересня 2024 р. № 1062 затверджено Порядок проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг[2]. Зазначеним документом визначено механізм оцінки відповідності суб'єктів, які мають намір надавати послуги електронної ідентифікації, надавачів послуг електронної ідентифікації, юридичних осіб, фізичних осіб - підприємців, які мають намір надавати кваліфіковані електронні довірчі послуги, кваліфікованих надавачів електронних довірчих послуг, центрального засвідчувального органу, засвідчувального центру та послуг, які вони надають, вимогам до надавачів послуг електронної ідентифікації, кваліфікованих надавачів електронних довірчих послуг, а також вимогам до послуг, які вони надають;

5) створення необхідних передумов (нормативних, організаційних, технологічних) для автентифікації користувачів сервісів цифрових послуг

[1] Стандарти кібербезпеки. Інтернет-сайт «VPN Unlimited». URL: https://www.vpnunlimited.com/ua/help/cybersecurity/cybersecurity-standards?srsltid=AfmBOopsfaN_s6MewFxLhG8qxVbsJIPqSM3RkTyOcc--LrrwidQ45iSu (дата звернення: 05.04.2025)

[2] Про затвердження Порядку проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг : Постанова Кабінету Міністрів від 13.09.2024 р. № 1062. *Урядовий портал.* URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-poriadku-provedennia-protsedury-otsinky-vidpovidnost-a1062.

(там, де це потрібно) за допомогою інтегрованої системи електронної ідентифікації з використанням технологій електронної ідентифікації та/або електронних довірчих послуг. Автентифікація – це процес перевірки справжності користувача за спроби доступу до системи чи сервісу, підтвердження того, що особа дійсно є тією, за кого себе видає. Без автентифікації безпеку цифрових послуг забезпечити неможливо. На сьогодні триває процес прийняття уніфікованих методів автентифікації для всіх міністерств і відомств;

6) підвищення ефективності системи захисту персональних даних громадян шляхом гармонізації законодавства України з відповідним законодавством ЄС та посилення відповідальності за порушення встановлених вимог безпеки цифрових послуг. Україна, відповідно до ст. 15 Угоди про асоціацію з ЄС, взяла на себе зобов'язання адаптувати своє законодавство у сфері захисту персональних даних до європейських стандартів[1]. Україною впродовж останніх двох років зроблено ряд кроків у цьому напрямі. Зокрема, було розроблено оновлену редакцію проєкту Закону про захист персональних даних № 5628 від 07.06.2021 року, який мав би суттєво зблизити національні норми з вимогами GDPR. Аналіз українського законодавства в контексті GDPR свідчить про необхідність подальшої гармонізації національних норм з європейськими стандартами захисту персональних даних. Проте, експерти зазначають, що існуючи розбіжності у сфері визначення відповідальності та механізмів контролю за цим процесом призводять до певної хаотичності процесу. Це негативно відбивається, перш за все, на українському бізнесу. За цих умов проблематично підвищувати довіру клієнтів, зміцнювати репутацію на міжнародному ринку та відкривати нові можливості для співпраці з європейськими партнерами на ринку цифрових послуг[2].

Упродовж останніх кількох років, Україна продовжує проводити значний плат роботи щодо практичної реалізації зазначених заходів задля захисту цифрових послуг, забезпечення кібербезпеки і протидії кіберзлочинності.

Висновки. На сьогодні правове забезпечення безпеки цифрових послуг в Україні є невід'ємною складовою політики держави у сфері кібербезпеки і протидії кіберзлочинності. Аналіз положень чинного національного законодавства про цифрові послуги дає підстави відзначити необхідність подальшої роботи з правової регламентації процедур досягнення безпечності і прозорості надання цифрових послуг, вчасне виявлення і нейтралізацію відповідних ризиків і загроз кібербезпеці. Відповідно, актуальним завданням юридичної науки є формування науково обґрунтованих пропозицій щодо інноваційного удосконалення правового

[1] Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Закон України від 16.09. 2014 р. № 1678-VII. *Відомості Верховної Ради України*. 2014 р. № 40. Ст. 2021.

[2] Кінаш М. Нові правила захисту персональних даних: як відповідати стандартам ЄС? *Юридична газета online*. URL: https://yur-gazeta.com/dumka-eksperta/novi-pravila-zahistu-personalnih-danih-yak-vidpovidati-standartam-es-.html (дата звернення: 20.04.2025).

забезпечення розвитку як самого ринку цифрових послуг, так і убезпечення національного цифрового середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про цифровий контент та цифрові послуги : Закон України від 10.08.2023 р. № 3321-IX. *Відомості Верховної Ради України*. 2023. № 90. Ст. 345.

2. Цифрові послуги в Україні: особливості регулювання сфери : повідомлення від 22.02.2024 р. *Інтернет-сайт «Ligazakon».* URL: https://biz.ligazakon.net/analitycs/225808_tsifrov-poslugi-v-ukran-osoblivost-regulyuvannya-sferi (дата звернення: 01.04.2025).

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. *Офіційний вісник України*. 2021. № 70. Ст. 4417.

4. Федоров М. Дії 3 роки. Як Україна отримала місце у світовій історії цифровізації? 14 лютого 2023. *Економічна правда*. URL: https://epravda.com.ua/columns/2023/02/14/697034/ (дата звернення: 28.03.2025).

5. Чорноус А. Г. Інформаційні ресурси як елемент національної інформаційної інфраструктури: їх створення та використання*. Інформація і право*. 2018. № 3. С. 49–55.

6. Стандарти кібербезпеки. *Інтернет-сайт «VPN Unlimited».* URL: https://www.vpnunlimited.com/ua/help/cybersecurity/cybersecurity-standards?srsltid=AfmBOopsfaN_s6MewFxLhG8qxVbsJIPqSM3RkTyOcc--LrrwidQ45iSu (дата звернення: 05.04.2025).

7. Про затвердження Порядку проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг : Постанова Кабінету Міністрів від 13.09.2024 р. № 1062. *Урядовий портал.* URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-poriadku-provedennia-protsedury-otsinky-vidpovidnost-a1062.

8. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09. 2014 р. № 1678-VII. *Відомості Верховної Ради України*. 2014 р. № 40. Ст. 2021.

9. Кінаш М. Нові правила захисту персональних даних: як відповідати стандартам ЄС? *Юридична газета online*. URL: https://yur-gazeta.com/dumka-eksperta/novi-pravila-zahistu-personalnih-danih-yak-vidpovidati-standartam-es-.html (дата звернення: 20.04.2025).

Стаття надійшла до редакції 20.04.2025

Oleksandr S. PEREDERII,
PhD in Law, Associate Professor
(Kharkiv National University V. N. Karazin, Kharkiv, Ukraine)

Lyudmila V. KULACHOK-TITOVA,
PhD in Law, Associate Professor
(Kharkiv National University V. N. Karazin, Kharkiv, Ukraine)

ORGANIZATIONAL AND LEGAL MEASURES TO ENSURING THE SECURITY OF DIGITAL SERVICES IN THE ASPECT OF COMBATING CYBERCRIME IN UKRAINE

The article, using methods of comprehensive analysis, presents a system of organizational and legal measures to ensure the security of digital services in terms of combating cybercrime in Ukraine. In particular, this includes strengthening the trust of the private sector and citizens in digital services provided by the state, unconditional fulfillment of requirements for ensuring cybersecurity and cyber protection during their provision, development of national information infrastructure, development of national standards in the field of cybersecurity, creation of bodies to assess the compliance of providers of electronic trust services with the requirements for qualified providers of qualified electronic trust services and authentication of their users, increasing the effectiveness of the system for protecting citizens' personal data by harmonizing the legislation of Ukraine with the relevant legislation of the European Union.

Based on the analysis of the provisions of the current legislative acts regulating state policy in the field of cybersecurity, as well as the processing of analytical materials on these issues, the content of measures to ensure digital services is disclosed, and attention is also focused on the existing problems of their full implementation. In particular, these are the issues of ensuring the security of users of the most state electronic applications, preserving the industry principle of informatization of state bodies, optimizing the architecture of information security management, which organizations and state authorities can create and use for their own protection, functional problems of the activities of bodies assessing the compliance of providers of electronic trust services with the established requirements, achieving unification of the process of applying authentication methods for all ministries and departments, the issue of achieving effective cooperation between European partners in the digital services market.

The position on the need for further work on legal regulation of procedures for achieving security and transparency in the provision of digital services, timely identification and neutralization of relevant risks and threats to cybersecurity is substantiated. Accordingly, the current task of legal science is to form scientifically based proposals for improving the legal support for the development of both the digital services market itself and the security of the national digital environment.

Key words: *Ukraine, cybersecurity, cybercrime, digital services, information*

infrastructure, legislation, European Union, legal innovations, countering cybercrime.