

К.І.С., 2015.220 с.

УДК 004.738.5:34(477:438)

**Плохотнюк А.А.**

*студентка третього курсу юридичного факультету  
Ягеллонський університет*

Науковий керівник:

**Заставна О.П**

*к.ю.н., старший викладач кафедри міжнародного та європейського права  
Західноукраїнський національний університет*

## **ВЗАЄМОЗВ'ЯЗОК ПРАВОВОЇ БЕЗПЕКИ В СЕРЕДОВИЩІ СУЧАСНИХ ТЕХНОЛОГІЙ (НА ПРИКЛАДАХ ПРОГРАМ ЕЛЕКТРОННОГО АДМІНІСТРУВАННЯ, ТАКИХ ЯК ДІЯ В УКРАЇНІ ТА MOVUWATEL І МОДУЛЬ УПРАВЛІННЯ СПРАВАМИ В ПОЛЬЩІ)**

У сучасному світі розвиток цифрових технологій істотно вплинув на форми здійснення публічного управління, та на механізми надання адміністративних послуг. Зараз у державах електронне адміністрування розглядається як ефективний інструмент реалізації прав громадян, підвищення доступності послуг і оптимізації діяльності органів державної влади. Водночас активне впровадження цифрових сервісів актуалізує питання правової безпеки, зокрема у сфері захисту персональних даних, стабільності функціонування державних інформаційних систем та протидії кіберзагрозам.

До впровадження цифрових рішень надання адміністративних послуг здійснювалося через значну кількість окремих органів та установ, таких як державна міграційна служба, центри надання адміністративних послуг, податкові органи, органи соціального захисту, пенсійний фонд, сервісні центри МВС, нотаріуси. Така модель передбачала особисту присутність заявника, використання паперових документів та багатоетапні адміністративні процедури, що створювало додаткові часові витрати та підвищувало ризик помилок і непотизму.

Запровадження цифрових сервісів призвело до зміни цієї моделі. В Україні ключову роль у цифровізації публічного адміністрування відіграє застосунок Дія, який забезпечує доступ до широкого спектра державних послуг у електронній формі. За допомогою цього застосунку громадяни можуть користуватися цифровими документами, подавати заяви до органів державної влади, отримувати довідки та витяги, підписувати документи з використанням електронного підпису, реєструвати підприємницьку діяльність, а також реалізовувати окремі цивільно-правові процедури в онлайн форматі [1].

Однак функціонування систем електронного адміністрування пов'язане також з ризиками кіберзагроз. До найбільш поширених належать атаки типу DDoS, спрямовані на порушення доступності сервісів, а також phishing та соціальна інженерія, які використовуються для отримання несанкціонованого доступу до внутрішніх систем. Окрему небезпеку становлять атаки на програмні інтерфейси, експлуатація невідомих вразливостей та довготривалі цілеспрямовані атаки, що можуть мати ознаки організованого або державного втручання [2].

З правової точки зору кібератаки на державні цифрові сервіси підлягають кримінальній відповідальності. В Україні такі діяння охоплюються нормами Кримінального кодексу України. Зокрема, стаття 361 передбачає відповідальність за несанкціоноване втручання в роботу інформаційних систем, натомість стаття 361-1 передбачає відповідальність за створення або розповсюдження шкідливого програмного забезпечення, стаття 362 передбачає відповідальність за зловживання доступом до інформації особами, які мають відповідні повноваження, а стаття 363-1 передбачає відповідальність за перешкоджання роботі електронних комунікаційних мереж [3]. Атаки на цифрові державні сервіси можуть також розглядатися в контексті загроз національній безпеці, особливо в умовах воєнного стану.

Як зазначають розробники Дії, важливим аспектом її функціонування є правова та технічна природа додатку. Застосунок не є окремою базою даних і не зберігає персональні дані користувачів на постійній основі. Він виконує функцію

цифрового інтерфейсу доступу до вже існуючих державних реєстрів. Отримання інформації відбувається лише у момент запиту через захищені канали зв'язку з використанням прикладних інтерфейсів програмування. Такий підхід відповідає принципам мінімізації обробки даних та обмеження доступу до приватної інформації користувачів відповідно до визначеної мети. Захист інформації в межах цифрових сервісів забезпечується шляхом використання сучасних криптографічних механізмів. Передача даних здійснюється із застосуванням протоколів шифрування, персональні дані зберігаються в державних реєстрах у зашифрованому вигляді, а доступ користувачів захищений механізмами автентифікації, зокрема біометричними засобами. Електронний підпис, який використовується в межах Дії, ґрунтується на застосуванні криптографічних ключів і дозволяє здійснювати юридично значимі дії без використання паперових носіїв [4].

Порівняльний аналіз польських електронних сервісів свідчить про застосування більш обмеженої моделі цифрового адміністрування. Застосунок mObywatel забезпечує доступ до цифрових документів, однак не охоплює повний цикл адміністративних процедур [5]. А сервіс Diia.PL орієнтований передусім на іноземців та надає інформаційний і сервісний доступ до окремих публічних послуг. Водночас Польща активно розвиває Moduł Obsługi Spraw спеціалізований електронний інструмент, який уже зараз дозволяє готувати та подавати онлайн-заяви на дозволи на тимчасовий і постійний побут для іноземців, з грудня 2025 року для багатьох категорій це є обов'язковим, та єдиним способом подання. Незважаючи на відмінності, як українська, так і польська моделі стикаються зі спільними викликами у сфері інформаційної та правової безпеки [6].

На тлі зростання кількості кіберінцидентів постає питання співвідношення ризиків і переваг цифрових сервісів. Аналіз практики їх функціонування свідчить, що на даний момент повна відмова від електронного адміністрування є неможливою. Цифрові сервіси забезпечують оперативність та доступність надання адміністративних послуг, що має істотне значення для реалізації прав

громадян, навіть в умовах перебування закордоном.

Отже, правова безпека в середовищі сучасних технологій має забезпечуватися шляхом поєднання технічних засобів захисту та ефективного правового регулювання. Криміналізація кібератак, контроль доступу до державних інформаційних систем і розвиток міжнародної співпраці у сфері кібербезпеки є необхідними елементами функціонування цифрової держави.

## ЛІТЕРАТУРА

1. Дія: електронні публічні послуги. Міністерство цифрової трансформації України. URL: <https://diia.gov.ua/>
2. Типи кібератак URL: <https://it-osvita.diia.gov.ua/task/item/4a074822-05ff-4a36-9c22-62d581b79717>
3. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III.
4. Міністерство цифрової трансформації України. URL: <https://thedigital.gov.ua/news/technologies/bezpeka-mobilnogo-zastosunku-diya>
5. Додаток 1. До регламенту про mObywatel URL: <https://www.gov.pl/attachment/1f6e31f6-8364-4eed-b5d8-8474d830a521>
6. Moduł Obsługi Spraw. URL: <https://www.mos.cudzoziemcy.gov.pl/en>

УДК 341.231.14

**Подубінська С.Р.**

*студентка третього курсу юридичного факультету*

*Ягеллонський університет*

Науковий керівник:

**Заставна О.П**

*к.ю.н., старший викладач кафедри міжнародного та європейського права*

*Західноукраїнський національний університет*

## ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ДОСТУПУ БІЖЕНЦІВ ДО МЕДИЧНОЇ ДОПОМОГИ В ПОЛЬЩІ

Охорона здоров'я, безсумнівно, є однією із найважливіших сфер діяльності сучасної держави; однією з базових функцій держави, що відображає стан