УДК 004.056:35.088.6:342.7
DOI https://doi.org/10.32782/pdu.2024.4.41

Р. О. Максимович
кандидат юридичних наук, докторант,
в.о. завідувача кафедри міжнародного та європейського права факультету міжнародних відносин
Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут»
ORCID ID: 0000-0003-1812-6624

КІБЕРБЕЗПЕКА В ЕЛЕКТРОННОМУ ВРЯДУВАННІ ЯК ЗАПОРУКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ СОЦІАЛЬНО ВРАЗЛИВИХ ВЕРСТВ НАСЕЛЕННЯ

Розвиток цифрових технологій та впровадження електронного врядування створюють нові можливості для покращення надання державних послуг, спрощення адміністративних процедур і підвищення прозорості в управлінні. Громадяни мають змогу отримувати доступ до державних послуг через інтернет, що значно підвищує ефективність взаємодії між державою та населенням. Однак із розвитком цих технологій постають нові виклики, зокрема в забезпеченні кібербезпеки.

Особливу увагу слід приділити захисту персональних даних у системах електронного врядування, оскільки їх використання в цифровому середовищі супроводжується високими ризиками витоку, маніпуляцій і незаконного використання. Порушення безпеки персональних даних може призвести до серйозних наслідків для громадян, включаючи порушення їхніх прав та безпеки. Враховуючи швидкий розвиток цифрових технологій, необхідно забезпечити надійний захист особистої інформації, що використовується в державних платформах.

Захист персональних даних є не лише технічним, а й соціальним завданням. На рівень кібербезпеки впливають різноманітні фактори, такі як цифрова грамотність громадян, доступ до технологій і ефективність контролю за інформаційними системами з боку держави. Важливим є постійне вдосконалення технічних заходів, таких як шифрування та багатофакторна автентифікація, а також забезпечення високого рівня обізнаності громадян щодо кіберзагроз та способів захисту своїх персональних даних.

Серед основних загроз кібербезпеки в контексті електронного врядування можна виокремити кібератаки, фішинг, злом баз даних та використання шкідливого програмного забезпечення. Такі загрози можуть негативно вплинути не лише на державні органи, але й на громадян, особливо на вразливі верстви населення, такі як пенсіонери та люди з інвалідністю. Вони часто мають обмежений доступ до цифрових ресурсів і недостатньо розвинену цифрову грамотність, що робить їх більш схильними до маніпуляцій з боку кіберзлочинців.

Тому важливо створювати системи підтримки для цих груп населення, навчати їх основам кібербезпеки, що дозволить зменшити ризики та підвищити рівень безпеки при взаємодії з державними платформами. У той самий час, державні органи повинні постійно оновлювати свої технології захисту і реагувати на нові кіберзагрози, розробляючи ефективні правові норми для обробки персональних даних і посилюючи контроль за їх збереженням.

Для ефективної боротьби з кіберзагрозами необхідно поєднувати технічні, правові та освітні заходи, що включають використання сучасних технологій шифрування, розробку національних стратегій кібербезпеки та регулярний моніторинг цифрових платформ.

Ключові слова: *кібербезпека, електронне врядування, захист персональних даних, цифрові технології, кіберзагрози.*

Постановка проблеми. Розвиток цифрових технологій та електронного врядування відкриває нові можливості для покращення доступу до державних послуг і спрощення адміністративних процедур, але зростаюча залежність від цифрових платформ ставить перед суспільством нові загрози у вигляді витоку і маніпуляцій персональними даними, що порушує права громадян. Особливо вразливими є соціально незахищені верстви населення, які мають обмежений доступ до технологій та недостатньо розвинену цифрову грамотність. Це вимагає комплексного підходу до забезпечення кібербезпеки, включаючи технологічні, правові та освітні заходи для збереження конфіденційності, справедливості та підвищення обізнаності громадян, що є необхідним для ефективного функціонування електронного врядування.

Аналіз останніх досліджень і публікацій. Останні дослідження в галузі електронного врядування та кібербезпеки підкреслюють важливість цифровізації судових процесів та забезпечення захисту персональних даних. Особливу увагу приділяється проблемам кібербезпеки, цифрової нерівності та захисту прав людини в умовах цифровізації. Дослідники, зокрема Ю. Кунєв, О. Панченко, Н. Кухарська, О. Мельник та В. Павліченко вносять значний вклад у розробку правових та етичних стандартів для безпечного використання цифрових технологій у державному управлінні.

Мета і завдання дослідження. Метою дослідження є вивчення проблеми забезпечення кібербезпеки в системах електронного врядування, зокрема у контексті захисту персональних даних, а також аналіз існуючих технологічних, правових і соціальних механізмів, спрямованих на зниження кіберризиків. Завданнями є оцінка сучасних загроз кібербезпеці в електронному урядуванні, вивчення ефективних методів захисту даних, розгляд етичних аспектів і правових норм у цій сфері, а також розробка рекомендацій щодо покращення захисту персональних даних та підвищення цифрової грамотності серед вразливих груп населення.

Виклад основного матеріалу. Розвиток цифрових технологій та впровадження електронного врядування відкривають нові можливості для покращення надання державних послуг, спрощення адміністративних процедур і забезпечення прозорості державного управління. Завдяки використанню сучасних інформаційних систем громадяни отримують доступ до державних сервісів безпосередньо через інтернет, що значно підвищує ефективність взаємодії між державою та суспільством.

Однак зростаюча залежність від цифрових платформ супроводжується серйозними викликами, пов'язаними з забезпеченням кібербезпеки. Використання персональних даних у цифровому середовищі створює ризики їх витоку, маніпуляцій, або незаконного використання, що може призвести до порушення прав громадян.

Таким чином, захист персональних даних у системах електронного врядування стає не лише технічним, а й соціальним викликом. Впровадження ефективних механізмів кібербезпеки, підвищення цифрової грамотності населення та посилення державного контролю за безпекою інформаційних систем є ключовими заходами для забезпечення захисту прав громадян у цифрову епоху [1].

Електронне врядування, як невід'ємна частина сучасної цифрової держави, включає низку державних послуг, що надаються через електронні платформи. Серед таких послуг можна назвати реєстрацію актів цивільного стану, оформлення соціальної допомоги, доступ до податкових та медичних послуг, а також багато інших важливих функцій, які спрощують та прискорюють взаємодію громадян з державними органами. Ці технології не лише сприяють зручності та доступності для громадян але й підвищують рівень прозорості та ефективності державного управління. Однак розвиток цифрових технологій супроводжується низкою нових загроз, які можуть мати серйозні наслідки для громадян і держави, якщо не забезпечити належний захист.

Одним із основних аспектів електронного врядування є надійний захист персональних даних. Ці дані можуть включати особисту інформацію громадян, медичні історії, банківські реквізити, дані

про податки, а також інші чутливі відомості, які потребують високого рівня захисту. У разі витоку або несанкціонованого доступу до такої інформації можуть виникнути серйозні юридичні та фінансові наслідки, зокрема, ризики фінансових шахрайств, крадіжки особистих даних та навіть загроза безпеці громадян [2].

Загрози кібербезпеці в контексті електронного врядування надзвичайно різноманітні, і включають кібератаки, фішинг, злом баз даних, використання шкідливого програмного забезпечення та інші методи несанкціонованого доступу. Кібератаки, зокрема, можуть мати на меті паралізацію роботи державних систем або незаконне використання персональних даних для злочинних цілей. У випадку фішингових атак зловмисники можуть намагатися отримати конфіденційну інформацію, маскуючись під легітимні органи влади або організації. Такі методи можуть ставити під загрозу не лише безпеку державних установ, але й персональні інтереси громадян, адже вони можуть бути введені в оману та потерпіти від шахрайських схем.

Особливо вразливими до кіберзагроз є соціально незахищені верстви населення, такі як пенсіонери, люди з інвалідністю, безробітні, діти та особи, що перебувають у складних життєвих обставинах. Ці групи часто мають обмежений доступ до цифрових технологій, а також недостатньо розвинуту цифрову грамотність, що робить їх більш вразливими до атак кіберзлочинців. Для багатьох з них розуміння основ кібербезпеки є значною проблемою, що відкриває простір для використання їхньої довіри та відсутності належних знань про захист даних. Наприклад, пенсіонери часто не мають досвіду в користуванні сучасними онлайн-сервісами та можуть не розпізнати фішингові листи чи інші шахрайські спроби.

Окрім того складність у забезпеченні кібербезпеки на рівні державних систем полягає в необхідності постійного оновлення технологій захисту, впровадження новітніх протоколів безпеки та навчання персоналу державних органів. У зв'язку з цим особливе значення має регулярне вдосконалення стратегій кіберзахисту, використання надійних методів шифрування та ідентифікації користувачів, а також безперервне підвищення обізнаності громадян про потенційні загрози та шляхи їх уникнення. Тільки завдяки комплексному підходу до кібербезпеки можна забезпечити належний захист даних і знизити ризики для соціально вразливих категорій населення [3].

Захист персональних даних є важливою складовою сучасного правового середовища, що забезпечує права та свободи громадян, а також підтримує довіру до цифрових систем і платформ. В умовах глобалізації та цифровізації суспільства питання захисту персональних даних набуває все більшої актуальності, оскільки нові технології відкривають нові можливості для збору, обробки та зберігання інформації, що стосується особистих даних громадян.

На міжнародному рівні важливим документом у сфері захисту персональних даних є Загальний регламент про захист даних (GDPR), ухвалений Європейським Союзом. Він встановлює високі стандарти безпеки даних та накладає зобов'язання на організації, що їх обробляють, незалежно від місця їхньої діяльності. Регламент передбачає такі права громадян, як право на доступ до власних даних, право на їх виправлення чи видалення, а також обов'язок компаній впроваджувати ефективні технічні й організаційні заходи для запобігання витокам інформації[4]. Окрім GDPR, важливу роль відіграє Директива NIS 2, яка спрямована на підвищення рівня кібербезпеки в державах ЄС. Вона встановлює вимоги до кіберзахисту критично важливих секторів, включаючи електронне врядування, банківську сферу, транспорт та охорону здоров'я, а також запроваджує заходи для запобігання кібератакам та реагування на них [5].

В Україні питання кібербезпеки врегульоване низкою нормативно-правових актів. Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи кіберзахисту, а також встановлює повноваження державних органів у цій сфері. Документ передбачає створення національної системи кібербезпеки, яка

включає органи державної влади, підприємства, установи та організації, відповідальні за протидію кіберзагрозам [6]. Важливу роль у захисті персональних даних відіграє також закон України «Про захист персональних даних», який встановлює вимоги до їх обробки, зберігання та передачі. Закон гарантує громадянам право на захист їхньої особистої інформації та передбачає санкції за порушення вимог щодо її обробки [7].

Забезпечення кібербезпеки в Україні здійснюється низкою державних органів, серед яких важливе місце посідає Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку). Вона відповідає за реалізацію державної політики у сфері кібербезпеки, забезпечення захисту державних інформаційних ресурсів та організацію взаємодії з міжнародними партнерами у сфері кіберзахисту. Ключову роль у боротьбі з кіберзлочинністю відіграє Кіберполіція України, яка займається розслідуванням злочинів у цифровій сфері, зокрема протидією фішингу, шахрайству, несанкціонованому втручанню в роботу електронних систем та іншим видам кіберзагроз.

Захист персональних даних та забезпечення стійкості електронного врядування до кіберзагроз вимагає постійного удосконалення нормативно-правової бази, розвитку технічних рішень та підвищення рівня цифрової грамотності серед населення. Впровадження міжнародних стандартів, посилення державного контролю та тісна співпраця між державними органами, приватним сектором і громадянським суспільством є ключовими факторами успішного розвитку кібербезпеки в електронному врядуванні.

Етичний аспект захисту даних є не менш важливим. Основними принципами є конфіденційність, справедливість та недискримінація. Прозорість обробки персональних даних і дотримання прав громадян допомагає забезпечити довіру до електронного врядування. Відповідальність за неправильне використання даних може призвести до серйозних наслідків, як юридичних, так і до зниження довіри до державних органів та цифрових платформ.

Особливу увагу слід приділити соціально незахищеним категоріям громадян, які можуть бути більш вразливими до несанкціонованого використання їхніх персональних даних. Для таких груп, як пенсіонери, люди з інвалідністю, діти, важливо забезпечити належний рівень захисту та доступ до навчання основам цифрової безпеки [8].

Загалом, захист персональних даних в електронному врядуванні є важливою складовою правової та етичної відповідальності державних органів і бізнесу. Це не лише юридичне зобов'язання, але й умова для розвитку довіри до цифрових технологій і забезпечення безпеки громадян в інформаційному середовищі.

Для ефективного захисту персональних даних у сфері електронного врядування необхідно впроваджувати комплексний підхід, що включає використання різноманітних технологічних рішень. Одним із основних заходів є шифрування даних, яке дозволяє запобігти несанкціонованому доступу до чутливої інформації. Шифрування забезпечує збереження конфіденційності навіть у разі перехоплення даних під час їх передачі між користувачем та державними платформами. Іншим важливим елементом є впровадження багатофакторної автентифікації. Ця технологія вимагає від користувачів проходити кілька етапів перевірки, що значно підвищує рівень безпеки доступу до електронних послуг. Вона включає, наприклад, поєднання пароля, смс-коду або біометричних даних, що ускладнює несанкціоноване проникнення в систему [9].

Не менш важливою складовою є розробка та впровадження національних стратегій кібербезпеки, які повинні забезпечити єдину систему захисту інформаційних ресурсів на рівні держави. Такі стратегії передбачають створення нормативно-правової бази, а також формування організаційних і технічних заходів для мінімізації ризиків кіберзагроз. Це включає визначення відповідальності за порушення кібербезпеки та забезпечення обміну інформацією між органами влади, бізнесом і громадянами. Регулярний моніторинг та аудит державних цифрових платформ є ще одним важливим

заходом для запобігання кіберзагрозам. Це дає змогу своєчасно виявляти вразливості в системах та усувати їх до того, як вони будуть використані зловмисниками. Постійний контроль за діяльністю інформаційних систем також дозволяє швидко реагувати на нові загрози і забезпечувати постійну підтримку належного рівня безпеки.

Не менш важливим аспектом є освітні програми з кіберграмотності для соціально вразливих категорій населення. Оскільки ці групи часто мають обмежений доступ до знань та ресурсів у сфері кібербезпеки, важливо забезпечити їх базовими знаннями, що дозволять їм безпечно користуватися цифровими платформами та захищати свої персональні дані від кіберзагроз. Навчання соціально вразливих верств населення допоможе знизити ризики для цих груп і сприяти їх інтеграції у цифрове суспільство [10].

Висновки. Розвиток електронного врядування значно спрощує взаємодію громадян з державою, забезпечуючи швидкий доступ до різноманітних послуг, проте ця трансформація також супроводжується викликами в сфері кібербезпеки. Зокрема, захист персональних даних стає надзвичайно важливим, оскільки зростає ризик їх несанкціонованого використання або витоку. Для належного забезпечення кібербезпеки необхідно впроваджувати комплексні технологічні рішення, включаючи шифрування даних, багатофакторну автентифікацію та розробку національних стратегій кібербезпеки. Крім того, особливу увагу слід приділяти підвищенню цифрової грамотності серед соціально вразливих груп населення, що дозволить їм безпечно користуватися цифровими платформами. Комплексний підхід, який поєднує технічні, правові та освітні заходи, стане основою для ефективного захисту прав громадян в цифровому середовищі, зміцнюючи довіру до електронного врядування і сприяючи його розвитку.

Список використаної літератури:

1. Rohrig W. Cyber Security and Cyber Defense in the European Union. Cyber Security Review 2014. №2. P. 7-16
2. Чуба Н. В. Розбудова електронного урядування: загрози та виклики. Публічне урядування. 2024. № 2 (39). С. 78–84.
3. Захист інформації в системах електронного урядування. Частина 13: посібник. Київ: ФОП Москаленко О.М., 2017. 72 с.
4. Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) URL : https://zakon.rada.gov.ua/laws/show/984_008-16#Text
5. NIS2 Directive: new rules on cybersecurity of network and information systems. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
6. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
7. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
8. Шадська У. Захист персональних даних: чому важливі етичні принципи під час цифровізації. URL: https://zmina.info/columns/zahyst-personalnyh-danyh-chomu-vazhlyvi-etychni-prynczypy-pid-chas-czyfrovizacziyi/
9. Дуравкін П. М., Гафич І. І. Сучасні виклики та майбутнє правового захисту персональних даних: під впливом розвитку цифровізації. Право та інновації. 2023. № 3 (43). С. 89-100.
10. Труш О. О. Забезпечення кібербезпеки при прийнятті рішень органами публічного управління. Державне будівництво. 2019. № 2. URL: http://nbuv.gov.ua/UJRN/DeBu_2019_2_23.

Maksymovych R. O. Cybersecurity in e-governance as a key to protecting personal data of socially vulnerable groups

The development of digital technologies and the implementation of e-government create new opportunities for improving the delivery of public services, simplifying administrative procedures, and increasing transparency in governance. Citizens can access public services via the internet, which significantly enhances the efficiency of interaction between the state and the population. However, with the development of these technologies, new challenges arise, particularly in ensuring cybersecurity.

Special attention must be paid to the protection of personal data in e-government systems, as its use in the digital environment is accompanied by high risks of leakage, manipulation, or illegal use. Breaches of personal data security can have serious consequences for citizens, including violations of their rights and safety. Given the rapid development of digital technologies, reliable protection of personal information used on government platforms is essential.

The protection of personal data is not only a technical but also a social issue. Various factors influence the level of cybersecurity, such as citizens' digital literacy, access to technologies, and the effectiveness of state control over information systems. Continuous improvement of technical measures, such as encryption and multi-factor authentication, as well as ensuring a high level of citizen awareness about cyber threats and ways to protect their personal data, are important.

Among the main cybersecurity threats in the context of e-government are cyberattacks, phishing, database hacking, and the use of malicious software. Such threats can negatively affect not only government bodies but also citizens, especially vulnerable groups such as pensioners and people with disabilities. These groups often have limited access to digital resources and insufficient digital literacy, making them more susceptible to manipulation by cybercriminals.

Therefore, it is crucial to create support systems for these groups of the population, teach them the basics of cybersecurity, and reduce risks while enhancing their security when interacting with government platforms. At the same time, government bodies must continually update their protection technologies and respond to new cyber threats by developing effective legal norms for processing personal data and strengthening control over its storage.

To effectively combat cyber threats, it is necessary to combine technical, legal, and educational measures, including the use of modern encryption technologies, the development of national cybersecurity strategies, and the regular monitoring of digital platforms.

Key words: *cybersecurity, e-governance, personal data protection, digital technologies, cyber threats.*