

УДК 004.658.6:004.056.53

DOI [https://doi.org/10.15589/znp2025.2\(500\).36](https://doi.org/10.15589/znp2025.2(500).36)STATE ELECTRONIC REGISTRY DATABASES:
ANALYSIS OF THE TERRITORIAL LOCATION OF SERVERSБАЗИ ДАНИХ ДЕРЖАВНИХ ЕЛЕКТРОННИХ РЕЄСТРІВ:
АНАЛІЗ ТЕРИТОРІАЛЬНОГО РОЗМІЩЕННЯ СЕРВЕРІВ**Olexander V. Zadereyko**

zadereyko@onua.edu.ua

ORCID: 0000-0003-0497-9861

Olena G. Trofymenko

trofymenko@onua.edu.ua

ORCID: 0000-0001-7626-0886

Svitlana E. Yelenych

o.yelenych@onua.edu.ua

ORCID: 0000-0003-4999-3034

Nataliia I. Loginova

loginova@onua.edu.ua

ORCID: 0000-0002-9475-6188

Volodymyr I. Hura

ihu@ukr.net

ORCID: 0009-0001-2166-5410

Olexander V. Troyanskiy

o.v.troyanskiy@op.edu.ua

ORCID: 0000-0001-9755-6010

О. В. Задерейко,

канд. техн. наук, доцент

О. Г. Трофименко,

канд. техн. наук, доцент

С. І. Єленич,

головний бібліограф наукової бібліотеки

Н. І. Логінова,

канд. пед. наук, доцент

В. І. Гура,

канд. техн. наук, доцент

О. В. Троянський,

канд. техн. наук, доцент

*National University "Odesa Law Academy", Odesa**Національний університет «Одеська юридична академія», м. Одеса*

Abstract. The article highlights the issues of protection and accessibility of databases of state electronic registers. Personal data of citizens of Ukraine of these databases are used in information-analytical and information-communication systems to optimize accounting and ensure the digital sovereignty of the state. During the war, there is a direct threat of losing personal databases of electronic registers due to constant cyber and physical attacks on the country's infrastructure. The *purpose* of the article is to study the physical location of the servers of the databases of the electronic registers of Ukraine, to analyze the possible impact on the security and accessibility of these registers of factors of different territorial placement of personal databases, both on the territory of the state during the war and abroad in order to preserve the functionality of the state's digital infrastructure. The research *methodology* consists in considering possible options for the location of databases of state electronic registers during martial law in the country; analyzing the advantages and disadvantages of each of the options for such location; checking the physical location of servers of databases of electronic registers; development of measures and recommendations that will ensure the uninterrupted operation of the state's digital infrastructure. *Results.* Under martial law, a balanced and reasonable approach to choosing the location of state registers will help minimize the threat of leaks, damage, distortion and loss of databases with personal data of citizens of Ukraine. An important aspect of such a choice is the creation of regularly updated backup copies of state register databases for the possible restoration of the operability of these registers in the event of damage to data centers during military operations. The analysis conducted allows us to assess in detail the risks and benefits of various options for the location of electronic state registers of Ukraine on servers for storing databases of personal data of citizens during military operations and to determine the most appropriate option.

Key words: databases; electronic registers; state registers; personal data; security of state registers.

Анотація. Статтю присвячено висвітленню питань захисту і доступності баз даних державних електронних реєстрів. Показано, що персональні дані громадян України цих баз даних використовуються в інформаційно-

аналітичних та інформаційно-комунікаційних системах з метою оптимізації ведення обліку та забезпечення цифрового суверенітету держави. З'ясовано, що за умов дії воєнного стану у цифровому середовищі держави є пряма загроза втрати баз персональних даних електронних реєстрів через постійні кібернетичні та фізичні атаки на інфраструктуру країни. *Метою статті* є дослідження фізичного розташування серверів баз даних електронних реєстрів України, аналіз можливого впливу на захищеність і доступність цих реєстрів факторів різного територіального розміщення баз персональних даних, як на території держави на під час війни, так і за кордоном задля збереження функціональності цифрової інфраструктури держави. *Методика* дослідження полягає в розгляді можливих варіантів розміщення баз даних державних електронних реєстрів під час дій воєнного стану в країні; аналізі переваг та недоліків кожного з варіантів такого розміщення; перевірці фізичного розташування серверів баз персональних даних електронних реєстрів; розробці заходів та рекомендацій, які забезпечать безвідмовну роботу цифрової інфраструктури держави. *Результати*. За умов дії воєнного стану виважений та розумний підхід до вибору розміщення державних реєстрів допоможе мінімізувати загрози витоку, пошкодження, спотворення та втрати баз даних з персональними даними громадян України. Немаловажним при такому виборі є створення на регулярній основі обновлюваних резервних копій баз даних державних реєстрів задля можливого відновлення працездатності цих реєстрів у разі пошкодження дата-центрів під час воєнних дій. Проведений аналіз дозволяє детально оцінити ризики та переваги різних варіантів розташування електронних державних реєстрів України на серверах для зберігання баз персональних даних громадян під час воєнних дій та визначити найбільш доцільний варіант.

Ключові слова: бази даних; електронні реєстри; державні реєстри; персональні дані; безпека державних реєстрів.

ПОСТАНОВКА ЗАДАЧІ

За умов стрімкого розвитку цифрової інфраструктури суспільства та впровадження веборієнтованих систем електронної взаємодії державних електронних інформаційних ресурсів гостро постало питання захисту баз даних цих систем від несанкціонованого доступу. Наразі до основних завдань діяльності міністерств, центральних і місцевих органів виконавчої влади належать надання інформаційних та інших послуг користувачам в мережі Інтернет із використанням електронних інформаційних систем. Крім того, сфери медицини, освіти, банківської справи, страхування, бібліотечної та архівної справ впроваджують та використовують цифрову інфраструктуру у вигляді реєстрів різного спрямування та баз персональних даних. Зростання обсягів персональних даних в державних реєстрах, обмін ними при взаємодії електронних систем державних інформаційних ресурсів, отримання та передача електронних копій документів, часте користування електронними послугами у повсякденному житті через мережу Інтернет створюють додаткові кіберризики та загрози у сфері безпеки персональних даних.

Підвищення рівня захисту персональних даних громадян є пріоритетним напрямком у сфері інформаційної безпеки держави, що зумовлено важливістю захисту приватності громадян, запобігання зловживанням, протидії кібератакам, підвищення рівня довіри до урядових та приватних інституцій, а також виконання міжнародних зобов'язань. Персональні дані містять багато чутливої інформації, яка є важливою для приватного життя кожної людини. Захист персональних даних допомагає запобігти несанкціонованому доступу до критичних інформаційних систем і ресурсів, знижує ризики фінансових махінацій та

інших форм шахрайства. Саме ефективний захист персональних даних підвищує рівень довіри громадян до державних та приватних інституцій, що важливо для збереження стабільності у суспільстві та ефективного функціонування економіки. Крім того, виконання міжнародних стандартів і законодавства щодо захисту персональних даних сприяє підтриманню міжнародного співробітництва і позитивного іміджу країни на міжнародній арені. Йдеться, перш за все, про реєстри та бази персональних даних громадян України, оскільки вони мають вирішальну роль у забезпеченні функціонування сфер державного управління, господарської діяльності, оподаткування, освіти, зайнятості населення, медицини, соціального захисту, пенсійного забезпечення, державної реєстрації речових прав на нерухоме і рухоме майно тощо. Ці обставини відіграють важливу роль у формуванні електронних ресурсів цифрового суспільства.

Важливим елементом структури безпеки державних реєстрів за умов війни є місце зберігання баз персональних даних громадян України, тобто їх фізичне розташування в безпечному енергонезалежному місці. Вибір місць для розташування дата-центрів, серверів і мережевих вузлів має ґрунтуватися на комплексному аналізі можливих глобальних наслідків вразливості цифрової та енергетичної інфраструктури держави, особливо за умов дії воєнного стану й прояву злочинних дій проти цифрової інфраструктури держави, а також при виникненні надзвичайних ситуацій техногенного та кліматичного характеру.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Дослідженню питань захищеності персональних даних приділяється значна увага у наукових публікаціях, але переважно вони не пов'язані з вивченням

впливу територіального розташування серверів, на яких розміщують бази даних державних реєстрів, на захист баз персональних даних від несанкціонованого доступу і ризиків порушення цілісності таких реєстрів. Так, науковці у роботі [1] досліджено стан основних українських електронних реєстрів і баз персональних даних України, які містять інформацію про населення країни. В дослідженні [2] проаналізовано електронні реєстри Данії, Швеції, Фінляндії, Норвегії, Нідерландах, Естонії, Франції. Аналіз досвіду України та зарубіжних країн свідчить про розвинені системи реєстрів охорони здоров'я, освіти, бізнесу, земельні кадастри і реєстри прав власності, які зберігають інформацію про громадян. Уся інформація передається через засоби зв'язку до центральних реєстрів, які використовуються для ухвалення рішень на державному рівні. Проте у дослідженнях [1–2] питання безпеки державних реєстрів розглядаються опосередковано, переважно з позиції їх правового регулювання. Робота [3] зосередилась на потребі змін нормативних підходів при розгляді питань територіальної юрисдикції в кіберпросторі. В статті [4] автори звертають увагу на різке зростання кількості витоків персональних даних у США протягом останніх кількох років і надзвичайну важливість захисту особистих фінансових даних людей. У роботі [5] автори, враховуючи як останні випадки збою та серйозні пошкодження дата-центрів, так і еволюцію міжнародних та європейських норм і стандартів, пропонують аналітичну методологію для оцінки територіальних факторів ризику для центрів оброблення даних у Мілані (Італія). Автори статті [6] досліджують особливості систем виявлення витоків даних у забезпеченні інформаційної безпеки на певному підприємстві, позаяк такі системи надають можливість моніторингу, виявлення та захисту конфіденційної інформації в реальному часі. Автор роботи [7] звертає увагу на те, що цілісність даних забезпечує точність, надійність та узгодженість даних протягом життєвого циклу, тоді як безпека даних стосується захисту даних від несанкціонованого доступу, модифікації, видалення чи крадіжки. У дослідженні [8] наголошується на зростанні складності кіберзагроз і мінливому ландшафті технологічних досягнень, які вимагають постійної адаптації та вдосконалення протоколів безпеки, а також на етичних міркуваннях, відзначаючи потребу переходу до більш етичних практик оброблення даних і важливість підтримки громадської довіри шляхом відповідального управління даними. Робота [9] досліджує критичні проблеми безпеки та конфіденційності даних у системах охорони здоров'я на основі інтернету речей (IoT) і радіочастотної ідентифікації (RFID), а також розглядає поточні рішення, зокрема методи шифрування, протоколи автентифікації та стратегії анонімізації даних. Автори статті [10] проаналізували питання кібербезпеки «розумного уряду» для впровадження

проекту «Розумне місто». В роботі [11] досліджено можливості технологій штучного інтелекту щодо покращення виявлення загроз та реагування на інциденти, при цьому автори наголошують на важливості розв'язання проблем, пов'язаних із прозорістю, упередженістю та етичними міркуваннями в алгоритмах штучного інтелекту. У статті [12] досліджено вплив рішень на основі штучного інтелекту на захист персональних даних і принципи рівності перед законами Індонезії, проаналізовано ці проблеми з точки зору позитивістської філософії, яка наголошує на суворому дотриманні законодавства та ефективному нагляді. Дослідження [13] вивчає питання кібербезпеки в оцифруванні державного управління, вразливості інфраструктури, зосереджуючись на навчанні співробітників і правових наслідках. У статті [14] проаналізовано фактори, які впливають на інформаційну безпеку підприємства. Усі фактори розділені на чотири групи: безпека, осередок безпеки, навчання та загрози. В роботі [15] продемонстровано структурну модель системи оцінювання кібербезпеки хмарних сервісів об'єктів інформаційної інфраструктури. Дослідження [16] пропонує інтеграцію блокчейн-технологій у проект «Дія» як ефективного засобу для підвищення конфіденційності та безпеки персональних даних. Аналіз наявних публікацій показує велику зацікавленість дослідників у питаннях безпеки інформаційних електронних систем, у тому числі щодо захищеності персональних даних. Також виявлено певний інтерес науковців до аналізу стану державних електронних реєстрів.

ВІДОКРЕМЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Питання важливості вибору місця зберігання баз даних при забезпеченні захисту баз персональних даних державних реєстрів залишаються малодослідженими та за умов воєнних дій і постійних кібератак потребують ґрунтового наукового дослідження.

МЕТА, ОБ'ЄКТ, ПРЕДМЕТ ТА МЕТОДИ ДОСЛІДЖЕННЯ

Метою статті є дослідження фізичного розташування серверів баз даних найбільш важливих електронних реєстрів України, аналіз можливого впливу на захищеність і доступність цих реєстрів факторів різного територіального розміщення баз персональних даних, як на території держави під час війни, так і за кордоном задля збереження функціональності цифрової інфраструктури держави.

Методи. Дослідження проводиться з використанням загальнонаукових методів дослідження, як-от: пошук, системний аналіз, спостереження, синтез, абстрагування та порівняння, абдукція, ідеалізація, пояснення та аналогія, історичний і логічний методи.

Об'єктом дослідження є бази даних державних електронних реєстрів.

Предметом дослідження є розташування серверів баз даних найбільш важливих електронних реєстрів України.

ОСНОВНИЙ МАТЕРІАЛ

У сучасній цифровій державі ефективне управління та належне функціонування досягається комплексним використанням електронних систем реєстрації громадян. Наразі ці системи інтегровані у складну інформаційну інфраструктуру у формі державних реєстрів різного спрямування [17]. На державному рівні відбувається постійний моніторинг і докладаються неабиякі зусилля задля покращення рівня захисту баз персональних даних таких реєстрів, а міжнародне співробітництво у сфері ідентифікації громадян сприяє розробці стандартів і протоколів, які забезпечуватимуть сумісність та інтеграцію з національними інформаційними та інформаційно-комунікаційними системами органів державної влади, органів місцевого самоврядування, суб'єктів та взаємовідносин користувачів у глобальному цифровому середовищі.

Порушення роботи електронних систем, реєстрів та баз персональних даних громадян є критичними для функціонування електронної держави, позаяк вони можуть зруйнувати її цифрову інфраструктуру й спричинити дестабілізацію суспільних відносин в державі через порушення прав і свобод її громадян. Серйозну загрозу цифровому суверенітету держави становить штучне створення тимчасової недоступності електронних реєстрів, внаслідок несанкціонованого доступу, блокування та пошкодження баз персональних даних громадян [18]. Стабільна робота взаємопов'язаних між собою електронних систем, реєстрів та баз персональних даних є важливою для забезпечення захисту прав і свобод громадян.

Суб'єкти (власники, розпорядники, уповноважені особи), які здійснюють оброблення персональних даних, зобов'язані на державному рівні забезпечувати захист баз персональних даних громадян від несанкціонованого доступу, копіювання, передачі, знищення, маніпулювання, блокування доступу до них. Наприклад, адміністрування, функціонування та

захист вебпорталу «Дія» забезпечує технічний адміністратор, а місцем зберігання персональних даних є інформаційно-комунікаційна система базових сервісів державного підприємства «ДІА» (ДІА.Enterprise.Cloud, <https://diia.gov.ua/policy>).

Важливим фактором збереження баз персональних даних від часткової або повної втрати є фізичне місце розташування серверів, на яких зберігаються бази персональних даних численних електронних державних реєстрів, позаяк перебої в їх енергопостачанні під час війни в Україні, створюють значні ризики щодо функціонування численних електронних реєстрів і систем [19]. Забезпечення максимального рівня захищеності баз персональних даних громадян України від їх знищення або пошкодження є невіддільною складовою безвідмовного функціонування сучасної цифрової інфраструктури держави.

Вибір місця територіального розташування серверів та пов'язаних з ними резервних копій, необхідних для оперативного відновлення доступу у разі пошкодження їх цілісності або втрати, є стратегічним для держави, оскільки це безпосередньо впливає на захищеність і доступність персональних даних громадян України [20]. Саме тому ця проблема набуває першочергового значення особливо під час воєнного стану в державі через можливі перебої в роботі енергогенеруючої та цифрової інфраструктури, зокрема серверів, що обслуговують електронні системи державних реєстрів.

Такі обставини зумовлюють потребу завчасного планування та проведення заходів для захисту та збереження електронних систем державних реєстрів, баз персональних даних громадян України та пов'язаних з ними резервних копій. Воно може бути реалізовано у різних напрямках (рис. 1):

1. Розташування державних електронних систем реєстрів на серверах, що належать державі.
2. Розташування державних електронних систем реєстрів на серверах, що розташовані в країнах, які мають спільні з Україною кордони.
3. Розташування державних електронних систем реєстрів на серверах, що розташовані на територіях країн інших континентів.



Рис. 1. Можливі варіанти розміщення електронних державних реєстрів України

4. Розташування державних електронних систем реєстрів на серверах держави і резервування їх копій на територіях країн, які мають спільні з Україною кордони і країн інших континентів.

Розташування електронних державних реєстрів на серверах на території України має значні переваги: можливість прямого контролю над інфраструктурою та даними; мінімальні витрати на передачу даних через швидкий доступ до даних; мінімізація ризиків, пов'язаних з міжнародними конфліктами. Проте внутрішнє розташування серверів (на території України) під час повномасштабної війни має високі ризики вразливості від фізичних атак, пошкодження та знищення інфраструктури серверів внаслідок воєнних дій. Не виключена втрата доступу до даних у разі захоплення території. Немаловажним є можливі перебої в електропостачанні інфраструктури через дії воєнного стану. Крім того, внаслідок кібератак з боку ворога дані можуть бути втрачені чи то скомпрометовані.

Розташування баз даних реєстрів на серверах у сусідніх країнах ЄС, з якими Україна підтримує дружні відносини, є гарною альтернативою для безпечного розміщення баз персональних даних. Проте, попри переваги високого рівня захисту даних за європейськими стандартами та законами, мінімальних ризиків фізичного знищення інфраструктури, міжнародної підтримки та можливості швидкого відновлення даних, таке розміщення потребує значних витрат на оренду інфраструктури, обслуговування та зберігання даних за кордоном. Через розміщення даних в країнах ЄС можливі юридичні ускладнення через різницю в законодавстві, потенційні юридичні обмеження та конфлікти між законами України та ЄС. Це може створити проблеми з контролем доступу та захистом даних. Ну і до того ж, при такому розміщенні не виключена можливість кібернападів з боку третіх країн, які мають інтереси в цьому регіоні.

Розташування серверів у країнах інших континентів має свої переваги та ризики. Для того розміщення характерним є відсутність ризику фізичної деструкції інфраструктури через віддаленість від зони конфлікту і можливість доступу до передових технологій безпеки та захисту даних. Але при цьому характерними є значні затримки в доступі до даних через велику географічну віддаленість та високі витрати на обслуговування та зберігання даних на віддалених серверах. При цьому не виключені потенційні проблеми з відповідністю законодавчих вимог щодо захисту даних, адже дані підпадають під закони та регуляції іншої країни, що може відрізнятися від законів України. Крім того, відносини між країнами можуть впливати на доступність та безпеку даних. У разі політичних конфліктів, дані можуть стати заручником у міждержавних суперечках. Також не виключено, що захист даних може бути недостатнім, порівняно з національними стандартами. Тобто є ризик несанкціонованого

доступу або використання даних сторонніми особами. Віддалене зберігання даних ускладнює контроль над їхнім фізичним розташуванням та управлінням.

Комбіноване розташування серверів на території України та за кордоном є певним компромісом. Перевагами такого розміщення серверів є забезпечення резервного копіювання та можливість відновлення даних у разі втрати працездатності основних серверів. Через розподіл даних по різних географічних регіонах є висока гнучкість у виборі найбезпечніших локацій для зберігання даних. Хоча при цьому залишаються як потенційні проблеми з узгодженням юридичних вимог та стандартів безпеки різних країн, так і високі витрати на управління й координацію між різними локаціями серверів. Крім того, виникає потреба використання більш складних систем для забезпечення синхронізації та доступу до даних.

Для аналізу даних про місцезнаходження баз даних державних реєстрів у роботі здійснено перевірку фізичного розташування серверів баз персональних даних, пов'язаних з найбільш важливими електронними реєстрами. Були використані спеціалізований сервіс Whois, який дозволяє отримувати інформацію про місцезнаходження IP-адрес, серверів або вебсайтів [21], та утиліта IPNetInfo, яка дозволяє знайти всю службову інформацію про IP-адресу: власника IP-адреси, назву країни/штату, діапазон IP-адрес, контактну інформацію тощо [22]. Результати виконаного дослідження наведені у табл. 1.

Аналіз даних табл. 1 надає розуміння характеру персональних даних громадян, які зберігаються у базах даних відповідних реєстрів, даних про соціальну, фінансову, фіскальну і господарську діяльність підприємців, громадських формувань, організацій та установ. Встановлено, що на час дослідження, територіально бази даних електронних державних реєстрів України розміщені як на території країни, так і в країнах ЄС та США. При чому переважна частина (63 %) такого розміщення зосереджена в Україні (рис. 2).

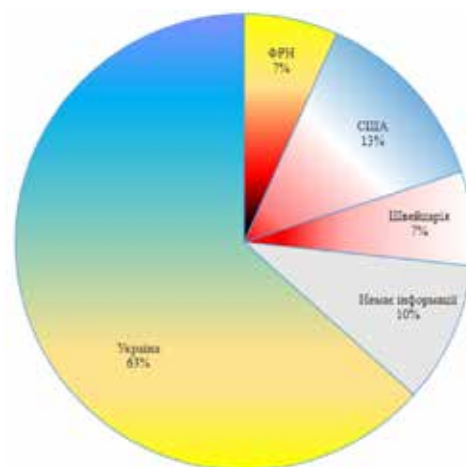


Рис. 2. Розподіл територіального розташування державних електронних реєстрів України

Таблиця 1. Територіальне розташування серверів реєстрів з базами персональних даних громадян України

№ з/п	Назва електронної системи	Джерела персональних даних громадян	Вебадреса	Власник по даних мережі	Розташування, IP-адреса
1	2	3	4	5	6
1.	Національні інформаційні системи (НАІС)	- Дані з базових реєстрів: Державний реєстр актів цивільного стану; Державний реєстр речових прав на нерухоме майно; Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань. - Суб'єкт персональних даних.	https://nais.gov.ua	Akamai Technologies, Inc.	США, Кембридж, 104.94.220.167
2.	Портал Дія – єдиний державний вебпортал електронних послуг	- Довідки з реєстрів. - Суб'єкт персональних даних.	https://diia.gov.ua	ORG-DD219-RIPE	Україна, Київ, 195.189.240.75
3.	Єдиний державний портал відкритих даних	- База персональних даних. - Суб'єкт персональних даних.	https://data.gov.ua	ORG-DD219-RIPE	Україна, Київ, 195.189.240.230
4.	Соціальний портал Міністерства соціальної політики України	- Дані з реєстру надавачів та отримувачів соціальних послуг. - Суб'єкт персональних даних.	https://soc.gov.ua/welcome	Microsoft Azure	Швейцарія, Цюрих, 20.203.140.132
5.	Портал Єдиної державної електронної системи у сфері будівництва	- Дані з базового реєстру будівель та споруд. - Суб'єкт персональних даних.	https://e-construction.gov.ua	ORG-DD219-RIPE	Україна, Київ, 195.189.240.138
6.	Система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта»	- База персональних даних. - Суб'єкт персональних даних.	https://trembita.gov.ua/	ORG-DD219-RIPE	Україна, Київ, 195.189.240.93
7.	Єдина державна електронна база з питань освіти (ЄДЕБО)	- Дані з: Реєстру документів про освіту; Реєстру студентських (учнівських) квитків; Реєстру сертифікатів зовнішнього незалежного тестування; Реєстру педагогічних, науково-педагогічних працівників. - База персональних даних. - Суб'єкт персональних даних.	https://info.edbo.gov.ua/	Patrolpolice-Datagroup	Україна, Київ, 80.91.162.219
8.	Інформаційно-комунікаційна система Українського центру оцінювання якості освіти (ІКС УЦОЯО)	Суб'єкт персональних даних.	https://testportal.gov.ua/	Interconnections-datagroup	Україна, Київ, 77.222.133.146
9.	Дія. Освіта	Суб'єкт персональних даних.	https://osvita.diia.gov.ua/	SE Diia	Україна, Київ, 195.189.240.104
10.	Електронна система охорони здоров'я (ЕСОЗ)	- До Центральної бази даних входять реєстри: Єдиний державний електронний реєстр пацієнтів; Реєстр декларацій про вибір лікаря; Реєстр медичних спеціалістів; Реєстр медичних працівників; Електронний реєстр лікарняних та інші реєстри. - Суб'єкт персональних даних.	https://moz.gov.ua/uk/elektronna-sistema-ohoroni-zdorovya	Cloudflare, Inc.	США, Сан-Франциско 104.18.8.180

Продовження таблиці 1

1	2	3	4	5	6
11.	Електронна система охорони здоров'я eHealth	- База персональних даних. - Суб'єкт персональних даних.	https://ehealth.gov.ua	Cloudflare, Inc.	США, Сан-Франциско, 104.18.8.180
12.	Інформаційно-комунікаційна система «Helsi»	- База персональних даних. - Суб'єкт персональних даних.	https://helsi.me/	Cloudflare, Inc.	США, Сан-Франциско, 172.67.8.57
13.	Національний репозиторій академічних текстів	- База персональних даних. - Суб'єкт персональних даних.	https://nrat.ukrintei.ua/	Private Joint Stock Company datagroup	Україна, Львів, 46.164.150.19
14.	Наука в Україні	- Портал реєстрів у сфері науки України. - База персональних даних. - Суб'єкт персональних даних.	https://nauka.gov.ua	ADA-MANT	Україна, Київ, 212.26.146.111
15.	Національна бібліотека України ім. В. І. Вернадського	- База персональних даних. - Суб'єкт персональних даних.	http://nbuv.gov.ua	State Enterprise Scientific and Telecommunication	Україна, Київ, 194.44.11.133.
16.	Електронні сервіси Державної служби України з питань геодезії, картографії та кадастру	- Надання відомостей з Державного земельного кадастру та інших реєстрів. - Суб'єкт персональних даних.	https://e.land.gov.ua	ADA-MANT	Україна, Київ, 212.26.131.137
17.	Портал електронних послуг Пенсійного фонду України	- Дані з: Реєстру застрахованих осіб; Електронного реєстру листків непрацездатності; Єдиного реєстру страхувальників. - Суб'єкт персональних даних.	https://portal.pfu.gov.ua/	Pensionfund-ua	Україна, Київ, 212.1.76.113
18.	Електронний кабінет Державної податкової служби України	- Дані з: Реєстру страхувальників; Реєстру платників єдиного податку; Реєстру платників ПДВ. - Суб'єкт персональних даних.	https://cabinet.tax.gov.ua/	State Tax Service of Ukraine	Україна, Дніпро, 193.200.32.30
19.	Національна бібліотека України імені Ярослава Мудрого	- База персональних даних. - Суб'єкт персональних даних.	https://nlu.org.ua/	SilverTelecom	Україна, Київ, 213.108.75.167
20.	Головний сервісний центр Міністерства внутрішніх справ	- Надання відомостей з Єдиного державного реєстру транспортних засобів. - Суб'єкт персональних даних.	https://hsc.gov.ua	Akamai Technologies	ФРН, Франкфурт, 2.18.64.33
21.	Сайт Міністерства фінансів України	- Дані з Реєстру відшкодування ПДВ. - Суб'єкт персональних даних.	https://mof.gov.ua	Akamai Technologies	ФРН, Франкфурт, 2.18.64.35
22.	Портал цифрового перетворення Е-Україна	- Дані з Державного реєстру виборців. - Суб'єкт персональних даних.	https://eukraine.org.ua/	Gigacloud	Україна, Київ, 185.168.131.174
23.	Е-ветеран	- Дані з Єдиного державного реєстру ветеранів війни. - Суб'єкт персональних даних.	https://eveteran.gov.ua/	Joint Ukrainian-German Enterprise INFOCOM	Україна, Ужгород, 212.1.101.172
24.	Інформаційно-обчислювальний центр Міністерства соціальної політики України	- Інформація за даними Єдиного державного реєстру отримувачів субсидій. - Суб'єкт персональних даних.	https://subsidi.ioc.gov.ua/	Microsoft Azure	Швейцарія, Цюрих, 20.208.28.40
25.	Паспортний сервіс ДП «Документ»»	Суб'єкт персональних даних.	https://passport.org.ua/	Cloudflare	Немає даних, 104.26.3.241
26.	Сервіси Державної митної служби України	- База персональних даних. - Суб'єкт персональних даних.	https://dmsu.gov.ua	Не має даних	Україна, немає даних, 194.42.203.6

Продовження таблиці 1

1	2	3	4	5	6
27.	Офіційний сайт Державної служби зайнятості України	- База персональних даних. - Суб'єкт персональних даних.	https://dcz.gov.ua/people	Joint Ukrainian-German Enterprise INFOCOM	Україна, Харків, 195.230.132.18
28.	Портал ведення реєстру територіальної громади	- Дані з реєстру територіальної громади. - Суб'єкт персональних даних.	https://rtg.dmsu.gov.ua/	Немає даних	Україна, немає даних, 194.42.203.7
29.	Моторне (транспортне) страхове бюро України	- Дані з Єдиної централізованої бази даних інформації про історію страхових випадків за договорами обов'язкового страхування цивільно-правової відповідальності. - Суб'єкт персональних даних.	https://mtsbu.ua/	Cloudflare	Немає даних, 104.21.89.45
30.	Онлайн-канали комунікації Газопостачальної компанії «Нафтогаз України»	- База персональних даних. - Суб'єкт персональних даних.	https://gas.ua/uk/home	Cloudflare	Немає даних, 172.64.149.103

ОБГОВОРЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Наразі Україна активно впроваджує цифрові рішення, що передбачають оброблення та збереження великої кількості персональних даних у державних системах, таких як «Дія», Реєстр виборців, Єдиний державний демографічний реєстр, податкові та медичні реєстри тощо. Важко переоцінити наявність та впровадження нових інформаційних платформ з надання електронних послуг громадянам України, адже це допомагає країні ефективніше реагувати на виклики воєнного стану та забезпечувати стабільність державних процесів. Цифрові рішення дозволяють швидше обробляти інформацію та ухвалювати рішення, що особливо важливо в умовах воєнного стану. Саме використання електронних інструментів дозволяє зменшити корупційні ризики та підвищити прозорість державних процесів. Цифрові рішення сприяють розвитку економіки, зокрема через підтримку малого та середнього бізнесу. Громадяни можуть отримувати державні послуги онлайн, що зменшує необхідність фізичної присутності та полегшує доступ до послуг. Цифрові системи мають забезпечувати надійний захист даних громадян, що особливо важливо в умовах війни.

Серед поширених і значимих загроз викрадення, пошкодження чи то знищення державних баз персональних даних є кібератаки з боку країни-агресора. Відбуваються регулярні атаки електронних систем державних реєстрів з метою порушення їхньої роботи або знищення даних. Прикладом такої атаки є масштабна зовнішня кібератака на державні реєстри 19 грудня 2024 року, в результаті якої постраждала робота Єдиних та Державних реєстрів, які перебувають у компетенції Міністерства юстиції України (<https://surf.li/zxwkcce>). Відновлення реєстрів потребувало тривалого часу і стало можливим, завдяки

наявним резервним копіям даних та високій кваліфікації фахівців відповідного профілю. Тому важливим напрямком захисту баз персональних даних є створення резервних дата-центрів розташованих як на території України, так і за її межами для мінімізації ризиків втрати даних, а також розвиток власних технологій зберігання та оброблення інформації.

Територіальне розташування серверів, що зберігають бази персональних даних громадян, має велике значення для їхнього захисту з різних причин. По-перше, розташування серверів у межах країни дає можливість застосувати національні закони та регуляції щодо захисту персональних даних. Коли дані зберігаються на серверах за кордоном, вони можуть підпадати під юрисдикцію інших країн, де закони про конфіденційність можуть бути менш жорсткими. Це створює ризики того, що дані можуть бути доступні для іноземних урядів або організацій. По-друге, локальне розташування серверів допомагає зменшити ризики кіберзагроз з інших країн. Сервери, розташовані в Україні, можуть бути краще захищені від атак, спрямованих на збирання чи компрометацію даних громадян. Зберігання даних в межах України дозволяє краще контролювати процеси зберігання, обробки та передачі даних, а також здійснювати аудит їхньої безпеки. Це допомагає забезпечити відповідність даних вимогам безпеки та конфіденційності. Фізичне розташування серверів на території України в мирний час дозволяє забезпечити їхню безпеку з точки зору фізичних загроз природних катастроф або фізичних вторгнень. Проте, коли на території країни йде війна і є ризик фізичного руйнування дата-центрів, захоплення територій, на яких вони розміщені, перебоїв з енергопостачанням, тоді варто переглянути підходи до розміщення серверів, які зберігають персональні дані громадян. У складних воєнних умовах важливо

забезпечити захист та доступність даних. В таких ситуаціях доцільно використовувати:

- *географічно розподілені резервні копії*: зберігання даних у різних географічних місцях зменшує ризик їхньої втрати через фізичне руйнування або перебої з енергопостачанням. Створення резервних копій в інших регіонах чи навіть країнах може допомогти зберегти дані надійно. При цьому важливо вибирати для зберігання резервних копій даних країни зі стабільними правовими системами та політичною стабільністю;

- *хмарні рішення*: використання хмарних сервісів може бути ефективним варіантом для зберігання даних, оскільки хмарні провайдери зазвичай мають високу стійкість до фізичних загроз і перебоїв з енергопостачанням. Хмарні рішення дозволяють швидко відновлювати дані в разі надзвичайних ситуацій. При виборі хмарних сервісів і провайдерів варто звертати увагу не тільки на вартість послуг, важливою є гарна репутація щодо здатності забезпечити високу надійність та відповідність вимогам безпеки;

- *захист даних*: забезпечення високого рівня шифрування даних як під час зберігання, так і під час передачі, дозволяє зберегти конфіденційність та захистити дані від несанкціонованого доступу [23]. Навіть якщо дані зберігаються за межами країни, їхній захист залишатиметься на високому рівні;

- *план аварійного відновлення*: розробка та впровадження плану аварійного відновлення, який включає чіткі інструкції з відновлення даних у разі фізичних руйнувань або перебоїв з енергопостачанням, допоможе забезпечити швидке повернення до нормальної роботи;

- *постійний аудит та оцінка ризиків*: регулярна перевірка безпеки зберігання та передачі даних допомагає усунювати вразливості системи, а оцінка ризиків, пов'язаних зі зберіганням даних, дозволяє вчасно виявляти потенційні загрози та вживати відповідних заходів для їхнього уникнення.

- *навчання персоналу*: забезпечення періодичного навчання персоналу на періодичній основі щодо безпеки даних та реагування на кіберзагрози є важливим для будь-якої цифрової інфраструктури, адже людський фактор залишається одним із найважливіших аспектів захисту даних. Більшість кібератак виникають через людські помилки. Це можуть бути неправильні налаштування систем безпеки, використання слабких паролів або відкриття фішингових листів. Зловмисники часто використовують методи соціальної інженерії, щоб обманом отримати доступ до конфіденційної інформації. Відсутність регулярного навчання та тренінгів з інформаційної безпеки може призвести до того, що працівники не будуть знати, як захистити себе та організацію від кібератак. Впровадження правильного регламенту безпеки та свідоме ставлення до інформаційної безпеки можуть знизити ризик

кібератак і забезпечити захист конфіденційної інформації в електронних державних реєстрах.

Запропоновані рекомендації можуть допомогти забезпечити надійність та безпеку персональних даних громадян навіть за важких умов дії воєнного стану в країні, адже питання захисту персональних даних громадян набуває критично важливого значення для національної безпеки України. Державні бази даних, що містять персональну інформацію громадян, є об'єктами підвищеної уваги з боку кібератак, несанкціонованого доступу та загроз фізичного знищення, а постійний розвиток інформаційних технологій спонукає до змін складових системи безпеки, політики конфіденційності електронних реєстрів щодо порядку оброблення персональних даних та обміну інформацією.

ВИСНОВКИ

Підвищення рівня захисту персональних даних громадян є пріоритетним напрямком у сфері інформаційної безпеки держави через постійне впровадження новітніх технологій оброблення та зберігання інформації, вдосконалення й оновлення програмного забезпечення, створення нових баз даних або їх інтегрування, змінення територіального місця розташування баз персональних даних або їх резервних копій. Сучасна цифрова трансформація суспільства супроводжується значними викликами у сфері захисту персональних даних громадян. Збільшення обсягу цифрових реєстрів та пов'язаних з ними баз персональних даних громадян, їх інтеграція та постійна взаємодія створюють певні ризики для захисту цифрової інфраструктури держави. Інтеграція державних реєстрів та їх взаємодія через електронні системи підвищують ефективність управління державою, але може створювати загрози витоку персональних даних громадян у разі несанкціонованого доступу.

Виконане дослідження довело, що територіальне розташування серверів, пов'язаних з базами персональних даних громадян України, є одним із ключових факторів їх захисту. Проведений аналіз дозволяє детально оцінити ризики та переваги різних варіантів розташування електронних державних реєстрів на серверах для зберігання баз персональних даних електронних державних реєстрів України під час воєнних дій та визначити найбільш доцільний спосіб їх захисту. Захист баз персональних даних громадян України потребує впровадження комплексного підходу, що включає нормативно-правове регулювання стосовно дозволу на тимчасове розміщення серверів баз персональних даних громадян України або їх резервних копій на територіях інших країн у безпечних юрисдикціях. Впровадження запропонованих у роботі заходів та рекомендацій дозволить гарантувати безвідмовну роботу цифрової інфраструктури держави, захистити персональні дані громадян, зберегти та значно зміцнити цифровий суверенітет України.

REFERENCES

- [1] Elektronni reistry: stan v Ukraini [Electronic registers: state in Ukraine]: col. monographs. (2021). / edited by O. Gladun, Kyiv: NAS of Ukraine, M.V. Ptukha Institute of Demography and Social Research, 636 p. [in Ukrainian].
- [2] Gladun, O., Pugacheva, M., Vynogradova, M. (2021). Elektronni reistry: yevropeyskyi dosvid stvorennia ta vykorystannia [Electronic registers: European experience in creation and use: collection of monographs], Kyiv: NAS of Ukraine, M. Ptukha Institute of Demography and Social Research, 271. [in Ukrainian].
- [3] Ryngaert, C. (2023), "Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts", *German Law Journal*, 24(3), 537–550. <https://doi.org/10.1017/glj.2023.24>.
- [4] Shafi, M., Fatima, M., Amna, M., Aryendra, D., Manish, V. (2024). Safeguarding Data Privacy: Enhancing Cybersecurity Measures for Protecting Personal Data in the United States. *Computer Security and Reliability*, 15, 1–19.
- [5] Gazzola, V., Menoni, S., Ghignatti, P., Marini, A., Mauri, R., Oldani, G. (2023). Analysis of Territorial Risks and Protection Factors for the Business Continuity of Data Centers. *Sustainability*, 15(7), 6005. <https://doi.org/10.3390/su15076005>.
- [6] Polotai, O., Puzyr, A. (2024). Analiz zasobiv zapobihannia vytohu konfidentsiinoi informatsii na pidpriemstvakh, na prykladi systemy DLP [Analysis of means of prevention of leakage of confidential information at enterprises, on the example of the DLP system]. *Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiedialnosti – Bulletin of Lviv State University of Life Safety*, 30, 134–144. <https://doi.org/10.32447/20784643.30.2024.13>. [in Ukrainian].
- [7] Duggineni, S. (2023). Impact of Controls on Data Integrity and Information Systems. *Science and Technology*, 13(2), 29–35. <https://doi.org/10.5923/j.scit.20231302.04>.
- [8] Sargiotis, D. (2024). Data Security and Privacy: Protecting Sensitive Information. *Data Governance. Springer, Cham*, 217–245. https://doi.org/10.1007/978-3-031-67268-2_6.
- [9] Olusegun, J., Ok, E., & Barnty, B. (2025). Data Security and Privacy Challenges in IoT and RFID-Based Healthcare Systems. <https://www.researchgate.net/publication/388891522>.
- [10] Baihaqi, M., Handayani, S., Sensuse, D., Lusa, S., Adi, P., Indriasari, S. (2024). Cybersecurity Implementation on Smart Government in Smart City: A Systematic Review. *International Journal on Advanced Science, Engineering and Information Technology*, 14, 1936–1943. <https://doi.org/10.18517/ijaseit.14.6.19874>.
- [11] Hudson, J. (2024). Revolutionizing Database Security with AI: Exploring the Latest Advances in Cybersecurity. *Database Security*, 23, 1–18. <https://doi.org/10.13140/RG.2.2.30396.24964>.
- [12] Chiang, D., Hoesin, Z. (2024). Ensuring Equality Before the Law and Personal Data Protection through Implementation of AI Integration in Single Identification Number Systems: A Positivism Philosophy Perspective. *Devotion. Journal of Research and Community Service*. 5(11), 1347–1361. <https://www.doi.org/10.59188/devotion.v5i11.20688>.
- [13] Sani, A., Olajide, A., Ogunsanya, V., Oyeboode, D., Alfred, J., Oseni, T., Jegede, E., Nwaogu, N., Abbas, R. (2025). Cybersecurity Challenges in Digitizing Government Administration. *Proceedings of the International Academy of Sciences*, Vol. 2(1), 1–13.
- [14] Bakayev, O., Suskyy, H. (2024). Metody zakhystu personalnoi informatsii v informatsiinykh systemakh [Methods of protecting personal information in information systems]. *Telekomunikatsiini ta informatsiini tekhnologii – Telecommunication and information technologies*, 2(83), 68–77. <https://doi.org/10.31673/2412-4338.2024.028190>. [in Ukrainian].
- [15] Ivanchenko, I., Pedchenko, Y. (2024). Strukturna model systemy otsiniuvannia kiberbezpeky khmarnykh servisiv obiektiv informatsiinoi infrastruktury [Structural model of the cybersecurity assessment system of cloud services of information infrastructure objects]. *Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika" – Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique"*. 1(25), 505–515. <https://doi.org/10.28925/2663-4023.2024.25.505515>. [in Ukrainian].
- [16] Balatska, V., Poberezhnyk, V. (2024). Kontseptsiiia zastosuvannia blokchein-tekhnologii dlia pidvyshchennia zakhyshchenosti personalnykh danykh platformy "Diya": vidpovidnist vymoham GDPR ta ukrainskomu zakonodavstvu [The concept of applying blockchain technologies to increase the security of personal data of the "Diya" platform: compliance with the requirements of the GDPR and ukrainian legislation]. *Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika" – Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique"*, 2(26), 268–290. <https://doi.org/10.28925/2663-4023.2024.26.681>. [in Ukrainian].
- [17] Kozhushko, O. (2021). Problemy ta perspektyvy rozvytku elektronnykh administrativnykh posluh v Ukraini [Problems and prospects of development of electronic administrative services in Ukraine]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriiia "Iurisprudentsiia" – Scientific Bulletin of the International Humanities University. Series: Jurisprudence*, 51, 46–51. <https://doi.org/10.32841/2307-1745.2021.51.9>. [in Ukrainian].
- [18] Zadereyko, A., Prokop, Y., Trofymenko, O., Loginova, N., Plachinda O. (2021), Development of an algorithm to protect user communication devices against data leaks. *Eastern-European Journal of Enterprise Technologies*, 1/2 (109), 24–34. <https://doi.org/10.15587/1729-4061.2021.225339>.
- [19] Zadereyko, O., Troyanskyi, O., Chanyshchev, R., Dyka, A. (2022). Kontseptualni osnovy zakhystu informatsiinoho suverenitetu Ukrainy [Conceptual foundations of protecting the information sovereignty of Ukraine]: the monograph; 2nd ed., revised and supplemented, Odesa: Phoenix, 220. <https://doi.org/10.32837/11300.22733>. [in Ukrainian].
- [20] Zadereyko O., Trofymenko, O., Loginova, N., Loboda, Y., Prokop, Y. (2024). Analiz potentsiinykh vytoziv personalnykh danykh u vebbrauzerakh [Analysis of potential personal data leaks in web browsers]. *Elektronne fakhove naukove vydannia*

“Kiberbezpeka: osvita, nauka, tekhnika” – Electronic Professional Scientific Journal “Cybersecurity: Education, Science, Technique”, 3(23), 199–212. <https://doi.org/10.28925/2663-4023.2024.23.199212>. [in Ukrainian].

- [21] Whois IP and domain lookup. Find and check IP address. <https://whoer.net/checkwhois>.
- [22] IPNetInfo: Retrieve IP Address Information from WHOIS servers. NirSoft. <https://www.nirsoft.net/utls/ipnetinfo.html>.
- [23] Zadereyko, O., Trofymenko, O., Prokop, Yu., Loginova, N., Dyka, A., Kukharensko, S. (2022). Research of potential data leaks in information and communication systems. *Radioelectronic and computer systems*, 4(104), 64–84. <https://doi.org/10.32620/reks.2022.4.05>.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

- [1] Електронні реєстри: стан в Україні : кол. моногр. / за ред. О.М. Гладуна; НАН України, Ін-т демографії та соціальних досліджень імені М. В. Птухи. Київ, 2021. 636 с.
- [2] Гладун О. М., Пугачова М. В., Виноградова М. В. Електронні реєстри: європейський досвід створення та використання: кол. моногр. НАН України, Ін-т демографії та соціальних досліджень імені М. В. Птухи. Київ, 2021. 271 с.
- [3] Ryngaert C. Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*. 2023. Vol. 24(3). P. 537–550. DOI: <https://doi.org/10.1017/glj.2023.24>
- [4] Shafi M., Fatima M., Amna M., Aryendra D., Manish V. Safeguarding Data Privacy: Enhancing Cybersecurity Measures for Protecting Personal Data in the United States. *Computer Security and Reliability*. 2024. Vol. 15. P. 1–19.
- [5] Gazzola V., Menoni S., Ghignatti P., Marini A., Mauri R., Oldani G. Analysis of Territorial Risks and Protection Factors for the Business Continuity of Data Centers. *Sustainability*. 2023. Vol. 15(7), 6005. DOI: <https://doi.org/10.3390/su15076005>.
- [6] Полотай О. І., Пузир А. О. Аналіз засобів запобігання витоку конфіденційної інформації на підприємствах, на прикладі системи DLP. *Вісник Львівського державного університету безпеки життєдіяльності*. 2024. № 30. С. 134–144. DOI: <https://doi.org/10.32447/20784643.30.2024.13>.
- [7] Duggineni S. Impact of Controls on Data Integrity and Information Systems. *Science and Technology*. 2023. Vol. 13(2). P. 29–35. DOI: <https://doi.org/10.5923/j.scit.20231302.04>.
- [8] Sargiotis D. Data Security and Privacy: Protecting Sensitive Information. In: Data Governance. Springer, Cham, 2024. Pp. 217–245. DOI: https://doi.org/10.1007/978-3-031-67268-2_6.
- [9] Olusegun J., Ok E., Barny B. Data Security and Privacy Challenges in IoT and RFID-Based Healthcare Systems. 2025. <https://www.researchgate.net/publication/388891522>
- [10] Baihaqi M., Handayani S., Sensuse D., Lusa S., Adi P., Indriasari S. Cybersecurity Implementation on Smart Government in Smart City: A Systematic Review. *International Journal on Advanced Science, Engineering and Information Technology*. 2024. Vol. 14. P. 1936–1943. DOI: <https://doi.org/10.18517/ijaseit.14.6.19874>.
- [11] Hudson J. Revolutionizing Database Security with AI: Exploring the Latest Advances in Cybersecurity. *Database Security*. 2024. Vol. 23. P. 1–18. DOI: <https://doi.org/10.13140/RG.2.2.30396.24964>.
- [12] Chiang, D., Hoesin, Z. Ensuring Equality Before the Law and Personal Data Protection through Implementation of AI Integration in Single Identification Number Systems: A Positivism Philosophy Perspective. *Devotion. Journal of Research and Community Service*. 2024. Vol. 5(11). Pp. 1347–1361. DOI: <https://www.doi.org/10.59188/devotion.v5i11.20688>.
- [13] Sani A., Olajide A., Ogunsanya V., Oyeboode D., Alfred J., Oseni T., Jegede E., Nwaogu N., Abbas R. Cybersecurity Challenges in Digitizing Government Administration. *Proceedings of the International Academy of Sciences*. 2025. Vol. 2(1). Pp. 1–13.
- [14] Бакаєв О. О., Суський Г. В. Методи захисту персональної інформації в інформаційних системах. *Телекомунікаційні та інформаційні технології*. 2024. № 2(83). С. 68–77. DOI: <https://doi.org/10.31673/2412-4338.2024.028190>.
- [15] Іванченко І., Педченко Є. Структурна модель системи оцінювання кібербезпеки хмарних сервісів об'єктів інформаційної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2024. № 1(25). С. 505–515. DOI: <https://doi.org/10.28925/2663-4023.2024.25.505515>.
- [16] Балацька В., Побережник В. Концепція застосування блокчейн-технологій для підвищення захищеності персональних даних платформи «Дія»: відповідність вимогам GDPR та українському законодавству. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2024. № 2(26). С. 268–290. DOI: <https://doi.org/10.28925/2663-4023.2024.26.681>.
- [17] Кожушко О. О. Проблеми та перспективи розвитку електронних адміністративних послуг в Україні. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція»*. 2021. № 51. С. 46–51. DOI: <https://doi.org/10.32841/2307-1745.2021.51.9>.
- [18] Zadereyko, A., Prokop, Y., Trofymenko, O., Loginova, N., Plachinda O. (2021). Development of an algorithm to protect user communication devices against data leaks. *Eastern-European Journal of Enterprise Technologies*. Vol. 1/2 (109). Pp. 24–34. DOI: <https://doi.org/10.15587/1729-4061.2021.225339>.
- [19] Концептуальні основи захисту інформаційного суверенітету України: монографія / О. В. Задерейко, О. В. Троянський, Р. І. Чанишев, А. І. Дика. 2-ге вид., перероб. і допов. Одеса: Фенікс, 2022. 220 с. DOI: <https://doi.org/10.32837/11300.22733>.
- [20] Задерейко О., Трофименко О., Логінова Н., Лобода Ю., Прокоп Ю. Аналіз потенційних витоків персональних даних у веббраузерах. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2024. № 3(23). С. 199–212. DOI: <https://doi.org/10.28925/2663-4023.2024.23.199212>.

- [21] Whois IP and domain lookup. Find and check IP address. URL: <https://whoer.net/checkwhois>
- [22] IPNetInfo: Retrieve IP Address Information from WHOIS servers. NirSoft. URL: <https://www.nirsoft.net/utis/ipnetinfo.html>
- [23] Zadereyko O., Trofymenko O., Prokop Yu., Loginova N., Dyka A., Kukharenko S. Research of potential data leaks in information and communication systems. *Radioelectronic and computer systems*. 2022. Vol. 4(104). Pp. 64–84. DOI: <https://doi.org/10.32620/reks.2022.4.05>.

© Задерейко О. В., Трофименко О. Г., Єленич С. І., Логінова Н. І., Гура В. І., Троянський О. В.
Дата надходження статті до редакції: 09.04.2025
Дата затвердження статті до друку: 22.04.2025