КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.735
УДК 004.658.6:004.056.53

Задерейко Олександр Владиславович
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія», Одеса, Україна
ORCID ID: 0000-0003-0497-9861
zadereyko@onua.edu.ua

Трофименко Олена Григорівна
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія», Одеса, Україна
ORCID ID: 0000-0001-7626-0886
trofymenko@onua.edu.ua

Єленич Світлана Іграфівна
головний бібліограф наукової бібліотеки
Національний університет «Одеська юридична академія», Одеса, Україна
ORCID ID: 0000-0003-4999-3034
o.yelenych@onua.edu.ua

Логінова Наталія Іванівна
кандидат педагогічних наук, доцент, завідувачка кафедри інформаційних технологій
Національний університет «Одеська юридична академія», Одеса, Україна
ORCID ID: 0000-0002-9475-6188
loginova@onua.edu.ua

Гура Володимир Ігорович
кандидат технічних наук, доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія», Одеса, Україна
ORCID ID: 0009-0001-2166-5410
ihu@ukr.net

СИСТЕМНИЙ АНАЛІЗ ЗАХИЩЕНОСТІ ДЕРЖАВНИХ ЕЛЕКТРОННИХ РЕЄСТРІВ ТА БАЗ ПЕРСОНАЛЬНИХ ДАНИХ

Анотація. В роботі розглянуто питання захисту баз персональних даних електронних державних реєстрів. Показано, що ці дані використовуються в інформаційно-аналітичних та інформаційно-комунікаційних системах з метою оптимізації ведення обліку та забезпечення цифрового суверенітету держави. З'ясовано, що за умов війни та поширення різних видів загроз з-посеред інших найбільш цінними і водночас вразливими щодо витоку персональних даних громадян є державні реєстри, портали електронних послуг, бази персональних даних державних організацій та установ. Штучне створення тимчасової недоступності електронних реєстрів, внаслідок несанкціонованого доступу, блокування та пошкодження баз персональних даних громадян становить серйозну загрозу цифровому суверенітету держави. Метою статті є системний аналіз критеріїв захисту баз даних електронних реєстрів громадян та розробка комплексної системи контролю доступу і захисту персональних даних у державних реєстрах. Розглянуто складові системи цифрової інфраструктури держави та роль взаємопов'язаних між собою електронних систем, реєстрів та баз персональних даних у забезпеченні прав і свобод громадян. Розроблено комплексну систему контролю доступу та захисту баз персональних даних, яка враховує різні варіанти можливого розміщення баз персональних даних, комунікаційні системи контролю доступу, можливі інструменти забезпечення захисту інформації та засоби запобігання витоку та втрати даних. Разом розглянуті складові формують комплексну систему контролю доступу та захисту персональних даних, яка не лише сприяє захищеності даних, а й забезпечує зручний і швидкий доступ до державних послуг для громадян. Для максимального ефекту важливо інтегрувати різні інструменти, системи контролю доступу і заходи безпеки, які допомагають забезпечити надійність та захищеність баз даних. Саме комплексний підхід до захисту баз персональних даних дозволяє мінімізувати

ризики витоку інформації та несанкціонованого доступу. Впровадження комплексної системи контролю доступу та захисту персональних даних для державних реєстрів є доцільним та необхідним кроком для забезпечення високого рівня захищеності інформації.

Ключові слова: захист даних; бази даних; персональні дані; електронні державні реєстри; бази персональних даних; контроль доступу; інформаційні технології; цифрова інфраструктура держави.

ВСТУП

Постановка проблеми. За умов інтенсифікації соціальної цифрової взаємодії, інтеграції електронних державних реєстрів та їхньої взаємодії через електронні системи відповідні бази з персональними даними стали одним з найцінніших ресурсів, а їх формування, накопичення, оброблення та використання є основою для забезпечення дієздатності цифрової сфери держави і суспільства. Відповідні бази даних електронних державних реєстрів містять відомості про громадян та осіб-мешканців країни. Саме ці дані дозволяють проводити аналіз стану суспільства в цілому та якість функціонування соціальної сфери. Прикладами таких реєстрів є: Єдиний державний демографічний реєстр; Державний реєстр виборців; Єдиний державний реєстр військовозобов'язаних; Реєстри територіальних громад; Єдиний державний реєстр декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування; Державний реєстр актів цивільного стану громадян; Спадковий реєстр; Державний реєстр речових прав на нерухоме майно; Єдиний державний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення; Єдиний реєстр боржників тощо. Так, Єдиний державний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення, зберігає дані про осіб, до яких застосовано заходи кримінально-правового характеру через вчинення корупційного правопорушення. Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань містить дані про зайнятість осіб. Спадковий реєстр, Державний земельний кадастр і Єдиний державний реєстр транспортних засобів є електронними базами даних, які містить відомості про майно громадян та їхні права на спадщину. В Єдину державну електронну базу з питань освіти взаємопов'язані різні реєстри системи освіти країни, серед яких: Реєстр документів про освіту, Реєстр суб'єктів освітньої діяльності, Реєстр здобувачів освіти, Реєстр студентських (учнівських) квитків, Реєстр сертифікатів педагогічних працівників, Реєстр сертифікатів зовнішнього незалежного оцінювання. Переоцінити важливість захищеності таких баз даних реєстрів складно, адже від їхньої цілісності залежить працездатність відповідних електронних систем і порталів, що забезпечує надійне функціонування цифрової сфери держави.

Саме на електронні бази даних реєстрів полюють зловмисники, вишукуючи їхні вразливості та способи їх зламу, викрадення або оприлюднення. Безпека й захист конфіденційної інформації в базах персональних даних державних реєстрів важливі для ефективного управління державою. Під час війни актуальність цих питань постає особливо гостро через стрімке зростання кількості кібератак, загроз та ризиків витоків персональних даних громадян шляхом несанкціонованого доступу, а відповідна інформація може бути використана для шпигунства чи то інших зловмисних цілей, аж до небезпеки збереження цифрового суверенітету держави.

Аналіз останніх досліджень та публікацій. Дослідженню питань захищеності персональних даних присвячені різні наукові публікації, але переважно вони не пов'язані з вивченням аспектів захисту баз персональних даних державних реєстрів від несанкціонованого доступу та ризиками порушення цілісності таких реєстрів. Так,

науковці у роботі [1] дослідили стан основних українських електронних реєстрів і баз персональних даних України, які містять інформацію про населення країни. В дослідженні [2] проаналізовано електроні 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 надходить до центральних реєстрів і надалі використовується для ухвалення рішень на державному рівні. Проте у дослідженнях [1], [2] питання безпеки державних реєстрів розглядаються опосередковано, переважно з позиції їх правого регулювання. В роботі [3] автори звертають увагу на різке зростання кількості витоків персональних даних у США протягом останніх кількох років і надзвичайну важливість захисту особистих фінансових даних людей. Автори статті [4] зосередили увагу на дослідженні особливостей 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 [5] 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 [6] наголошується на зростанні складності кіберзагроз і на 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 [7] 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 [8] проаналізували питання кібербезпеки «розумного уряду» для впровадження проєкту «Розумне місто». В роботі [9] 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 [10] 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 [11] вивчає питання кібербезпеки в оцифруванні державного управління, вразливості інфраструктури, зосереджуючись на навчанні співробітників і правових наслідках. У статті [12] проаналізовано фактори, які впливають на інформаційну безпеку підприємства. Усі фактори розділені на чотири групи: безпека, осередок безпеки, навчання та загрози. В роботі [13] продемонстровано структурну модель системи оцінювання кібербезпеки хмарних сервісів об'єктів інформаційної інфраструктури. Дослідження [14] пропонує інтеграцію блокчейн-технологій у проєкт «Дія» як ефективного засобу для підвищення конфіденційності та безпеки персональних даних. Аналіз наявних публікацій показує велику зацікавленість дослідників у питаннях безпеки інформаційних систем підприємств, у тому числі щодо захищеності персональних даних. Також виявлено певний інтерес науковців до аналізу стану державних електронних реєстрів. При цьому питання забезпечення комплексного захисту баз персональних даних державних реєстрів залишаються малодослідженими та за умов постійних кібератак потребують ґрунтовного наукового дослідження.

Метою статті є системний аналіз критеріїв захисту баз даних електронних реєстрів громадян та розробка комплексної системи контролю доступу і захисту персональних даних у державних реєстрах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В Україні належний рівень захисту персональних даних в процесі їх оброблення забезпечується виконанням вимог національного законодавства, а саме: Конституції України, Указу Президента «Про Доктрину інформаційної безпеки України», законів України: «Про національну безпеку України», «Про інформацію», «Захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», «Про електронні комунікації», «Про цифровий контент та цифрові послуги» «Про публічні електронні реєстри», Наказу Міністерства цифрової трансформації України від 20.05.2020 р. «Про затвердження Порядку обробки та захисту персональних даних, власником яких є Міністерство цифрової трансформації України», Порядку електронної (технічної та інформаційної) взаємодії, та інших нормативно-правових актів), європейських та міжнародних стандартів, ратифікованих Україною (Угоди про асоціацію між Україною та Європейським Союзом, Європейським співтовариством з атомної енергії та їх державами-членами, Угоди між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021–2027), Хартії Європейського Союзу про основоположні права, Договору про функціонування Європейського Союзу (ЄС), Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, Загального регламенту про захист даних — General Data Protection Regulation (GDPR) та інших документів), стандартів інформаційної безпеки (наприклад, Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, Положення про захист інформації в Національній системі масових електронних платежів та інших нормативних актів), вимог нормативних документів з питань технічного та операційного захисту інформації (зокрема, захисту персональних даних). Важливо завчасно оцінювати ризики, передбачати ситуації та наслідки, які можуть настати через потенційні кібератаки та вразливість баз персональних даних громадян, розташованих у межах цифрової інфраструктури держави.

Реєстри в Україні об'єднані в єдину систему електронної взаємодії державних електронних інформаційних ресурсів на базі платформи «Трембіта», Єдиного державного вебпорталу відкритих даних, Єдиного державного вебпорталу електронних послуг «Портал Дія». Деякі групи реєстрів об'єднані за сферою, наприклад: охорона здоров'я (Електронна система охорони здоров'я eHealth), освіта (Єдина державна електронна база з питань освіти) тощо. Облік всіх електронних реєстрів, кадастрів, класифікаторів, а також систем, які забезпечують їх функціонування та використовують інформацію з них, ведеться у Національному реєстрі електронних інформаційних ресурсів» (https://se.diia.gov.ua/nreir). Оператором всіх державних даних України є державне підприємство «Національні інформаційні системи» (https://nais.gov.ua/). Функціонування цифрової інфраструктури держави базується на інтеграції та взаємодії інформаційних систем, що поєднують системи електронних державних реєстрів, реєстрів органів виконавчої влади та місцевого самоврядування, територіальних громад, портали електронних послуг, зокрема портал Дія, баз персональних даних установ та організацій, а також інших інформаційних ресурсів, які містять персональні дані громадян [15].

Формування цифрової інфраструктури держави забезпечується функціонуванням таких важливих взаємопов'язаних складових системи (рис. 1):

- цифрове суспільство, сформоване на повсюдному використанні інформаційних технологій, включаючи сфери освіти, науки, культури, медицини, соціального забезпечення та трудових відносин, а також звичайного життя громадян;
- цифрова держава, яка охоплює сфери електронного врядування, електронних та адміністративних послуг, електронного документообігу, відкритих даних, публічних електронних реєстрах, національних електронних інформаційних ресурсів тощо;
- цифрове громадянство, яке формується у процесі життя та діяльності громадян в електронному середовищі, що забезпечується використанням інформаційних технологій;
- цифрова економіка, яка базується на впровадженні цифрових технологій у діяльність підприємств, використанні систем електронних платежів, розвитку електронної комерції та IT-індустрії, створенні інформаційно-комунікаційних систем та інформаційно-консультативних платформ для підтримки бізнесу тощо;
- цифровий суверенітет, який враховує особливості правового регулювання процесів трансформації інформаційного простору держави та посилення безпеки в цифровому світі, захисту персональних даних громадян та конфіденційної інформації на європейському, національному, державному та територіальному рівнях.

Рис. 1. Складові цифрової інфраструктури держави

За критичних умов функціонування цифрового суспільства та поширення різних видів загроз під час війни з-посеред інших найбільш цінними і водночас вразливими щодо витоку персональних даних громадян є державні реєстри, портали електронних послуг [16], бази персональних даних державних організацій та установ [17]. Задля захисту персональних даних постійно моніторяться і вдосконалюються інтегровані системи цифрової ідентифікації громадян на території України та за її межами, модернізуються підходи до забезпечення конфіденційності та захисту персоналізованої інформації в автоматизованих системах методом шифрування або знеособлення даних [12], пропонується застосування блокчейн-технологій для захисту документообігу та обміну інформацією [18], відбувається зберігання інформації державних реєстрів України засобами хмарних технологій, як один із засобів захисту персональних даних [19], а також впроваджуються заходи організаційного та технічного характеру щодо попередження витоку або несанкціонованого доступу до них.

До особливо чутливих відносять персональні та біометричні дані, пов'язані зі сферами фінансів та банківської справи, здоров'я, нерухомості, рухомого майна, пенсійного забезпечення та соціального захисту, расового та етнічного походження, політичних переконань тощо. Розголошення такої інформації може призвести до серйозних наслідків та завдати шкоди громадянам, суспільству та державі. Зокрема, витоки персональних даних створюють значні ризики порушення прав і свобод громадян, оскільки вони можуть бути використані в комерційних цілях, для політичної чи психологічної маніпуляції, шахрайства та інших зловмисних дій [20]. Тому захист персональних даних від кібератак на державні та публічні реєстри, бази персональних даних є одним з актуальних викликів в епоху цифрової трансформації суспільства.

Проведений системний аналіз різних чинників і факторів, які можуть впливати на захищеність баз даних державних реєстрів дозволив розробити комплексну систему контролю доступу та захисту баз персональних даних, структуру якої наведено на рис. 2.

Рис. 2. Комплексна система контролю доступу та захисту персональних даних

Системний підхід до безпеки баз персональних даних державних реєстрів забезпечують різні фактори:

1) ***Місце розташування баз даних***, тобто територіальне розташування серверів, що зберігають бази персональних даних, має велике значення для їхнього захисту з різних причин, серед яких: законодавче регулювання та юрисдикційна захищеність щодо захисту персональних даних, безпека від фізичних загроз (природних катастроф, фізичних вторгнень), контроль процесів зберігання, оброблення та передачі даних, а також аудит їхньої безпеки. Вибір місця для розташування дата-центрів, серверів та мережевих вузлів ґрунтується на комплексному аналізі глобальних наслідків вразливості цифрової та енергетичної інфраструктури держави при вчиненні військової агресії, злочинних дій проти

її цифрової інфраструктури, а також при виникненні надзвичайних ситуацій техногенного та кліматичного характеру. Територіальне розташування серверів, що зберігають бази персональних даних громадян, може бути організовано в різних місцях:

- *зберігання даних у межах країни* дозволяє застосовувати національні закони та державні стандарти захисту даних. Наприклад, в Україні діють закони, які захищають дані громадян, тому зберігання даних на території країни дозволяє краще контролювати безпеку їх персональних даних. Саме локальне розташування бази даних дозволяє забезпечити фізичний захист серверів, включаючи захист від природних катастроф та фізичних загроз. Проте під час війни зберігання даних у різних географічних місцях зменшує ризики їхньої втрати через можливе фізичне руйнування або перебої з енергопостачанням. В такому разі створення резервних копій в інших регіонах чи навіть країнах може допомогти зберегти дані безпечно. З іншого боку розташування бази даних у країні знижує ризики кіберзагроз з-за кордону та дозволяє ефективніше реагувати на кібератаки;
- *зберігання даних на серверах на території країн ЄС* регулюється його законодавством. Розміщення баз персональних даних громадян за кордоном має свої переваги, ризики та виклики, особливо у разі війни. ЄС має стабільні та надійні інфраструктури й технології для зберігання даних. Високий рівень захисту даних в ЄС забезпечують строгі законодавчі вимоги GDPR щодо захисту персональних даних. Близькість до європейських ринків може сприяти швидкому та ефективному доступу до даних для європейських партнерів. З іншого боку, наразі в деяких країнах ЄС спостерігаються діаметрально протилежні зміни політичних уподобань серед виборців, а отже зміни політичних лідерів країн і як наслідок можливі погіршення стосунків між країнами. Політична нестабільність ЄС може спричинити політичні чи то економічні кризи, які можуть вплинути на доступ до даних;
- при *зберіганні даних на серверах на території країн з інших континентів* вони підпадають під юрисдикцію цих країн, де закони про конфіденційність можуть бути менш жорсткими. Це створює ризики того, що дані можуть бути доступні для іноземних урядів або організацій. Далеко не всі країни мають такі строгі закони про захист даних, як в ЄС, а отже рівень захисту даних в них є нижчим. Варто враховувати можливу політичну нестабільність в тих чи інших країнах, що може вплинути і на безпеку даних на серверах відповідних країн. Крім того, відстань і різні часові пояси можуть ускладнювати доступ до даних.

2) Кожен з можливих ***інструментів забезпечення захисту інформації*** може забезпечити захищеність баз даних державних реєстрів, залежно від конкретних потреб та умов використання, а саме:

- *шифрування* забезпечує конфіденційність і цілісність інформації під час її передачі та зберігання, перетворюючи її на незрозумілий формат;
- *криптографія* застосовує математичні методи для захисту даних, гарантуючи їхню цілісність та конфіденційність;
- *механізм консенсусу* допомагає досягти узгодженість даних та взаємодію між системами задля уникнення конфліктів і забезпечення цілісності інформації;
- *сховище даних* забезпечує безпечне зберігання великих обсягів даних, підтримуючи їхню доступність і цілісність;

- *однорангова мережа* (peer-to-peer, P2P) дозволяє безпечну передачу даних між вузлами без централізованого сервера, зменшуючи ризики витоку;
- *вузол* як елемент мережі забезпечує обмін та зберігання даних;
- *технологія блокчейн* створює надійні, незмінні записи даних, гарантує їхню конфіденційність та цілісність;
- *знеособлення та де-знеособлення даних* забезпечує анонімність користувачів, що сприяє захисту їхніх персональних даних.

3) ***Засоби запобігання витоку та втрати інформації*** в їх комплексному застосуванні можуть значно підвищити рівень захищеності баз персональних даних державних реєстрів, знижуючи ризики витоку та втрати інформації. Для досягнення максимального ефекту важливо поєднувати різні заходи захисту та постійно оновлювати системи безпеки відповідно до нових загроз, як-от:

- *мережеве екранування* (Firewall) забезпечує захист мережі шляхом блокування несанкціонованих доступів та моніторингу трафіку. Використання сучасних фаєрволів допомагає захистити бази даних від зовнішніх кіберзагроз [21];
- *системи запобігання витоку даних* (Data Leak Prevention, DLP) дозволяють контролювати потоки даних, виявляти та попереджати несанкціоновані передачі конфіденційної інформації. Це дозволяє знизити ризики витоку даних через різні канали зв'язку (електронна пошта, USB-пристрої тощо) [22];
- *програмно-апаратні комплекси для оброблення і зберігання даних* забезпечують високу ступінь захисту даних під час їх оброблення та зберігання;
- *програмно-технічний контроль за фізичним захистом даних* контролює доступ до приміщень, де зберігаються сервера, моніторинг дій співробітників, відеоспостереження та інші заходи для забезпечення фізичної безпеки даних;
- *локальні системи захисту даних* дозволяють захистити дані на рівні окремих пристроїв та користувачів. Це поєднує антивірусне програмне забезпечення, шифрування твердих дисків, контроль доступу та інші засоби;
- *резервне копіювання даних* дозволяє зберегти дані у разі їх втрати або пошкодження. Важливо також забезпечити захист самих резервних копій, використовуючи шифрування та ізольоване зберігання;
- *додаткові джерела енергозабезпечення* (Uninterruptible Power Supply, UPS) допомагають уникнути втрати даних під час перебоїв з електропостачанням, забезпечуючи безперебійну роботу серверів та іншої критично важливої цифрової інфраструктури.

4) ***Комунікаційні системи контролю доступу*** відіграють важливу роль у забезпеченні захищеності баз персональних даних державних реєстрів. Сприяти підвищенню рівня захисту можуть:

- *електронна ідентифікація* дозволяє точно встановити особу користувача, зменшуючи ризики несанкціонованого доступу. Це особливо важливо для забезпечення безпеки державних реєстрів, де зберігаються чутливі персональні дані;
- *автентифікація* гарантує, що доступ до інформації отримують тільки авторизовані користувачі. Використання двофакторної автентифікації (2FA) або багатофакторної автентифікації (MFA) значно підвищує рівень безпеки, оскільки вимагає наявності кількох рівнів захисту (паролі, токени, SMS-коди тощо);

- *біометрична верифікація* (відбитки пальців, сканування обличчя або райдужної оболонки ока) для верифікації користувачів додає додатковий рівень безпеки, оскільки ці дані важко підробити. Біометрична верифікація забезпечує точну ідентифікацію та мінімізує ризики несанкціонованого доступу;
- система *BankID* дозволяє користувачам автентифікуватися через свій банк. Оскільки банки мають високі стандарти безпеки, використання BankID для доступу до державних реєстрів забезпечує додатковий рівень захисту. BankID дозволяє легко інтегрувати банківські механізми безпеки в державні системи;
- електронний *портал «Дія»* дозволяє громадянам України отримувати державні послуги онлайн. Впровадження такого сервісу підвищує рівень зручності та безпеки, оскільки доступ до нього здійснюється через захищені канали, використовуючи електронну ідентифікацію та автентифікацію.

Разом розглянуті складові формують комплексну систему контролю доступу та захисту персональних даних, яка не лише сприяє захищеності даних, а й забезпечує зручний і швидкий доступ до державних послуг для громадян. Для максимального ефекту важливо інтегрувати різні інструменти, системи контролю доступу і заходи безпеки, які допомагають забезпечити надійність та захищеність баз даних. Саме комплексний підхід до захисту баз персональних даних дозволяє мінімізувати ризики витоку інформації та несанкціонованого доступу.

Порушення роботи електронних систем, реєстрів та баз персональних даних громадян стають критичними для функціонування електронної держави. Такі випадки можуть зруйнувати її цифрову інфраструктуру та викликати дестабілізацію суспільних відносин в державі, 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. Стабільна робота взаємопов’язаних між собою електронних систем, реєстрів та баз персональних даних є важливою для забезпечення функціонування захисту прав і свобод громадян.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Розроблена комплексна система контролю доступу та захисту персональних даних для державних реєстрів є важливим кроком для забезпечення належного рівня безпеки та збереження інформації. Враховуючи місце розташування баз даних, можна оптимально використовувати національні закони та стандарти захисту даних, щоб забезпечити кращий контроль і фізичну безпеку даних. Локальне зберігання даних дозволяє підвищити рівень захисту завдяки близькості до користувачів і зменшенню ризиків, пов’язаних з зовнішніми загрозами. Використання резервних копій у різних географічних локаціях забезпечує додатковий рівень захисту, що особливо актуально за умов війни.

Забезпечення конфіденційності та цілісності даних можна досягти через шифрування та криптографічні методи, що гарантуватиме надійність інформації під час передачі та зберігання. Технології блокчейн та механізм консенсусу дозволять підтримувати узгодженість та незмінність даних, що є важливим для державних реєстрів. Інструменти запобігання витоку та втрати інформації, наприклад, мережеве екранування та системи DLP, допоможуть мінімізувати ризики кіберзагроз та несанкціонованого доступу до даних. Програмно-апаратні комплекси та резервне копіювання забезпечать високу ступінь захисту і відновлення даних у разі їх втрати. Додаткові джерела енергозабезпечення сприятимуть

безперебійній роботі серверів та іншого критично важливого обладнання, що дозволить уникнути втрат даних через перебої з електропостачанням.

Комунікаційні системи контролю доступу, серед яких електронна ідентифікація, автентифікація та біометрична верифікація, забезпечать точну ідентифікацію користувачів та зменшать ризики несанкціонованого доступу. Використання систем BankID та «Дія» підвищать рівень безпеки, завдяки інтеграції банківських механізмів захисту та забезпеченню захищених каналів доступу.

Загалом впровадження комплексної системи контролю доступу та захисту персональних даних для державних реєстрів є доцільним та необхідним кроком для забезпечення високого рівня безпеки інформації. Подальший розвиток системи має бути спрямований на постійне оновлення заходів захисту відповідно до нових загроз, а також інтеграцію нових технологій для підтримки безпеки даних на найвищому рівні. Важливо забезпечити навчання персоналу та користувачів щодо безпечного використання системи, аби мінімізувати людський фактор як потенційне джерело загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Electronic registers: state in Ukraine: col. Monographs.* (2021). Kyiv: NAS of Ukraine, M.V. Ptukha Institute of Demography and Social Research. https://www.idss.org.ua/arhiv/registers3.pdf
2. Gladun, O. M., Pugacheva, M. V., & Vynogradova, M. V. (2021). *Electronic registers: European experience in creation and use: collection of monographs.* Kyiv: NAS of Ukraine, M. V. Ptukha Institute of Demography and Social Research. https://idss.org.ua/arhiv/registers.pdf
3. 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.*
4. Polotai, O., & Puzyr, A. (2024). Analysis of means of prevention of leakage of confidential information at enterprises, on the example of the DLP system. *Bulletin of Lviv State University of Life Safety, 30,* 134–144. https://doi.org/10.32447/20784643.30.2024.13.
5. 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
6. Sargiotis, D. (2024). Data Security and Privacy: Protecting Sensitive Information. *In: Data Governance,* 217–245. Springer. https://doi.org/10.1007/978-3-031-67268-2_6
7. Olusegun, J., Ok, E., & Barnty, B. (2025). *Data Security and Privacy Challenges in IoT and RFID-Based Healthcare System*s. https://www.researchgate.net/publication/388891522
8. 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
9. Hudson, J. (2024). Revolutionizing Database Security with AI: Exploring the Latest Advances in Cybersecurity. *Database Security, 23.* https://doi.org/10.13140/RG.2.2.30396.24964
10. 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
11. Sani, A., Olajide, A., Ogunsanya, V., Oyebode, 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, 2(1),* 1–13. https://www.doi.org/rpc/2025/rpc.pias/00123 13
12. Bakayev, O. O. & Suskyy, H. V. (2024). Methods of protecting personal information in information systems. *Telecommunication and Informative Technologies, 2(83),* 68–77. https://doi.org/10.31673/2412-4338.2024.028190
13. Ivanchenko, I. & Pedchenko, Y. (2024). Structural model of the cybersecurity assessment system of cloud services of information infrastructure objects. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 1(25),* 505–515. https://doi.org/10.28925/2663-4023.2024.25.505515

14. Balatska, V., & Poberezhnyk, V. (2024). 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. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 2(26),* 268–290. https://doi.org/10.28925/2663-4023.2024.26.681
15. Zadereyko, O. V., Troyanskyi, O. V., Chanyshev, R. I., & Dyka, A. I. (2022). *Conceptual foundations of protecting the information sovereignty of Ukraine: monograph; 2nd ed., revised and supplemented*. Odesa: Phoenix. https://doi.org/10.32837/11300.22733
16. Dmytryshyn, M. V. & Zhurakivska, M. I. (2020). Leakage of personal data in electronic governance: realities and problems of state websites and portals. *Public management and administration in Ukraine, 20,* 111–119. https://doi.org/10.32843/pma2663-5240-2020.20.20
17. Gorodianska L., & Tsiukalo L. (2021). Information security of small businesses in the context of digitalization. *Collection of Scientific Works of the Military Institute of Kyiv National Taras Shevchenko University, (70),* 105–114. https://doi.org/10.17721/2519-481X/2021/70-11
18. Dziundziuk, B. (2023). Using blockchain technology as infrastructure in public sector. *Electronic scientific journal "Derzhavne upravlinnya: udoskonalennya ta rozvytok", 4,* 1–18. http://doi.org/10.32702/2307-2156.2023.4.9
19. Pazyuk, A. & Slabko, T. (2024). *Using commercial cloud technologies for processing data from state registers of Ukraine. IFES* Ukraine. https://www.ifesukraine.org/wp-content/uploads/2024/01/ifes-ukraine-the-use-of-commercial-cloud-technologies-for-processing-data-from-state-registers-of-ukraine-1.pdf
20. Zadereyko, O., Trofymenko, O., Prokop, Yu., Loginova, N., Dyka, A., & Kukharenko, 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
21. 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
22. Zadereyko O., Trofymenko, O., Loginova, N., Loboda, Y., & Prokop, Y. (2024). Analysis of potential personal data leaks in web browsers. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 3(23),* 199–212. https://doi.org/10.28925/2663-4023.2024.23.199212

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Olexander Zadereyko
PhD, Associate Professor
Associate Professor at the Department of Information Technologies
National University "Odessa Law Academy", Odesa, Ukraine
ORCID ID: 0000-0003-0497-9861
zadereyko@onua.edu.ua

Olena Trofymenko
PhD, Associate Professor
Associate Professor at the Department of Information Technologies
National University "Odessa Law Academy", Odesa, Ukraine
ORCID ID: 0000-0001-7626-0886
trofymenko@onua.edu.ua

Svitlana Yelenych
Chief Bibliographer of the Scientific Library
National University "Odessa Law Academy", Odesa, Ukraine
ORCID ID: 0000-0003-4999-3034
o.yelenych@onua.edu.ua

Nataliia Loginova
PhD, Associate Professor
Head of the Department of Information Technologies
National University "Odesa Law Academy", Odesa, Ukraine
ORCID ID: 0000-0002-9475-6188
loginova@onua.edu.ua

Volodymyr Hura
PhD, Associate Professor
Associate Professor at the Department of Information Technologies
National University "Odessa Law Academy", Odesa, Ukraine
ORCID ID:0009-0001-2166-5410
ihu@ukr.net

SYSTEMATIC ANALYSIS OF THE SECURITY OF STATE ELECTRONIC REGISTERS AND PERSONAL DATABASES

Abstract. The paper considers the issue of protecting personal databases of electronic state registers. These data are used in information and analytical and information and communication systems in order to optimize record keeping and ensure the digital sovereignty of the state. During war and the danger of various types of threats, the most valuable and at the same time vulnerable to leakage of personal data of citizens are state registers, portals of electronic services, databases of personal data of state organizations and institutions. Inaccessibility of electronic registers due to unauthorized access, blocking and damage to personal databases of citizens poses a serious threat to the digital sovereignty of the state. The purpose of the article is a systematic analysis of the criteria for protecting databases of electronic registers of citizens and the development of a comprehensive system of access control and protection of personal data in state registers. The components of the state digital infrastructure system and the role of interconnected electronic systems, registers and personal data bases in ensuring the rights and freedoms of citizens are considered. A comprehensive system of access control and protection of personal databases has been developed. This system considers various options for placing personal data bases, communication access control systems, possible tools for ensuring information security and means for preventing leakage and loss of data. The combination of components forms a comprehensive system of access control and personal data protection, which not only promotes data security, but also provides convenient and fast access to government services for citizens. For maximum effect, it is important to integrate various tools, access control systems and security measures that help ensure the reliability and security of databases. A comprehensive approach to protecting personal databases allows minimizing the risk of information leakage and unauthorized access. The

implementation of a comprehensive system of access control and protection of personal data for state registers is an appropriate and necessary step to ensure a high level of information security.

Keywords: data protection; databases; personal data; electronic state registers; personal databases; access control; information technologies; digital infrastructure of the state.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Electronic registers: state in Ukraine: col. Monographs.* (2021). Kyiv: NAS of Ukraine, M.V. Ptukha Institute of Demography and Social Research. https://www.idss.org.ua/arhiv/registers3.pdf
2. Gladun, O. M., Pugacheva, M. V., & Vynogradova, M. V. (2021). *Electronic registers: European experience in creation and use: collection of monographs.* Kyiv: NAS of Ukraine, M. V. Ptukha Institute of Demography and Social Research. https://idss.org.ua/arhiv/registers.pdf
3. 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.*
4. Polotai, O., & Puzyr, A. (2024). Analysis of means of prevention of leakage of confidential information at enterprises, on the example of the DLP system. *Bulletin of Lviv State University of Life Safety, 30,* 134–144. https://doi.org/10.32447/20784643.30.2024.13.
5. 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
6. Sargiotis, D. (2024). Data Security and Privacy: Protecting Sensitive Information. *In: Data Governance,* 217–245. Springer. https://doi.org/10.1007/978-3-031-67268-2_6
7. Olusegun, J., Ok, E., & Barnty, B. (2025). *Data Security and Privacy Challenges in IoT and RFID-Based Healthcare System*s. https://www.researchgate.net/publication/388891522
8. 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
9. Hudson, J. (2024). Revolutionizing Database Security with AI: Exploring the Latest Advances in Cybersecurity. *Database Security, 23.* https://doi.org/10.13140/RG.2.2.30396.24964
10. 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
11. Sani, A., Olajide, A., Ogunsanya, V., Oyebode, 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, 2(1),* 1–13. https://www.doi.org/rpc/2025/rpc.pias/00123 13
12. Bakayev, O. O. & Suskyy, H. V. (2024). Methods of protecting personal information in information systems. *Telecommunication and Informative Technologies, 2(83),* 68–77. https://doi.org/10.31673/2412-4338.2024.028190
13. Ivanchenko, I. & Pedchenko, Y. (2024). Structural model of the cybersecurity assessment system of cloud services of information infrastructure objects. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 1(25),* 505–515. https://doi.org/10.28925/2663-4023.2024.25.505515
14. Balatska, V., & Poberezhnyk, V. (2024). 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. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 2(26),* 268–290. https://doi.org/10.28925/2663-4023.2024.26.681
15. Zadereyko, O. V., Troyanskyi, O. V., Chanyshev, R. I., & Dyka, A. I. (2022). *Conceptual foundations of protecting the information sovereignty of Ukraine: monograph; 2nd ed., revised and supplemented*. Odesa: Phoenix. https://doi.org/10.32837/11300.22733
16. Dmytryshyn, M. V. & Zhurakivska, M. I. (2020). Leakage of personal data in electronic governance: realities and problems of state websites and portals. *Public management and administration in Ukraine, 20,* 111–119. https://doi.org/10.32843/pma2663-5240-2020.20.20
17. Gorodianska L., & Tsiukalo L. (2021). Information security of small businesses in the context of digitalization. *Collection of Scientific Works of the Military Institute of Kyiv National Taras Shevchenko University, (70),* 105–114. https://doi.org/10.17721/2519-481X/2021/70-11

18. Dziundziuk, B. (2023). Using blockchain technology as infrastructure in public sector. *Electronic scientific journal "Derzhavne upravlinnya: udoskonalennya ta rozvytok", 4,* 1–18. http://doi.org/10.32702/2307-2156.2023.4.9
19. Pazyuk, A. & Slabko, T. (2024). *Using commercial cloud technologies for processing data from state registers of Ukraine. IFES* Ukraine. https://www.ifesukraine.org/wp-content/uploads/2024/01/ifes-ukraine-the-use-of-commercial-cloud-technologies-for-processing-data-from-state-registers-of-ukraine-1.pdf
20. Zadereyko, O., Trofymenko, O., Prokop, Yu., Loginova, N., Dyka, A., & Kukharenko, 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
21. 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
22. Zadereyko O., Trofymenko, O., Loginova, N., Loboda, Y., & Prokop, Y. (2024). Analysis of potential personal data leaks in web browsers. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 3(23),* 199–212. https://doi.org/10.28925/2663-4023.2024.23.199212