УДК 004.42:658.8
DOI https://doi.org/10.32782/IT/2024-4-4

Володимир БОГОМ'Я
доктор технічних наук, професор, професор кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
***ORCID:** 0000-0003-4403-3130*
***Scopus Author ID:** 51863292100*

Любов ЧЕРЕМІСІНА
викладач кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
***ORCID:** 0009-0005-0719-0745*

Андрій ЯРМОЛАТІЙ
викладач кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна
***ORCID:** 0009-0004-8655-9928*

Бібліографічний опис статті: Богом'я, В., Черемісіна, Л., Ярмолатій, А. (2024). Безпечна обробка даних в бізнес-інтернет платформах та системах електронної комерції. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 29–36, doi: https://doi.org/10.32782/IT/2024-4-4

БЕЗПЕЧНА ОБРОБКА ДАНИХ В БІЗНЕС-ІНТЕРНЕТ ПЛАТФОРМАХ ТА СИСТЕМАХ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Глобалізація та розвиток мережі інтернет докорінно змінили способи електронної комерції та бізнес-платформ ставши рушійною силою сучасного суспільства. Інтернет перетворився на універсальну платформу для інтеграції бізнесів, наукових спільнот і громадян світу, забезпечуючи безпрецедентний рівень взаємодії та доступу до комерційних послуг.

Проте стрімке поширення інформаційних технологій несе із собою й суттєві ризики. Зокрема, питання захисту чутливих даних користувачів, які можуть бути викрадені, втратити конфіденційність або навіть використані для маніпуляцій, стали центральними у сфері інформаційної безпеки. Це загрожує не лише окремим користувачам, але й підриває довіру до цифрових сервісів у цілому, що перешкоджає їхньому подальшому розвитку.

***Мета роботи.** Розгляд досвіду і викликів практичного впровадження стандартів резиденції даних в бізнес платформах, які мають клієнт-серверну архітектуру, що мають відповідати сучасним вимогам захисту систем електронної комерції.*

***Методологія дослідження.** В роботі використані емпіричні та теоретичні методи.*

***Наукова новизна.** Проаналізовано основні технічні підходи для забезпечення відповідності вимогам щодо резиденції даних в бізнес-інтернет платформах та системах електронної комерції, а сам: географічне розміщення серверів, шифрування та токенізація, обмеження доступу та проксі-сервери.*

Відсутність єдиних підходів до визначення чутливих даних і механізмів їх захисту створює ситуації, коли особиста інформація користувачів стає вразливою. Розв'язання цих проблем вимагає створення та удосконалення міжнародних стандартів регулювання захисту даних, які будуть враховувати особливості глобального цифрового середовища та сприяти гармонізації національних законодавств.

***Висновки.** В статті наведено, що питання резиденції даних залишається одним з головних технічних і юридичних викликів сьогодення для сучасного бізнесу та систем електронної комерції, де основним каменем спотикання є сама клієнт-серверна архітектура сучасних веб-платформ та інших додатків цієї ж архітектури, які працюють в глобальній мережі.*

***Ключові слова:** системи електронної комерції, мережа Інтернет, захист даних, обробка даних, безпека інформації, бізнес-інтернет платформа, кібербезпека.*

Volodymyr BOHOMYA
Doctor of Technical Sciences, Professor, Professor at the Department of Cyber Security, Information Technologies and Economics, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, bog260341@gmail.com
***ORCID:** 0000-0003-4403-3130*
***Scopus Author ID:** 51863292100*

Liubov CHEREMISINA
Lecturer at the Department of Cybersecurity, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, cheremisina1112@gmail.com
***ORCID:** 0009-0005-0719-0745*

Andrii YARMOLATII
Lecturer at the Department of Cybersecurity, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, ayarmolatii@gmail.com
***ORCID:** 0009-0004-8655-9928*

To cite this article: Bohomya, V., Cheremisina, L., Yarmolatii, A. (2024). Bezpechna obrobka danykh v biznes-Internet platformakh ta systemakh elektronnoi komertsii [Secure data processing in business-Internet platforms and e-commerce systems]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 29–36, doi: https://doi.org/10.32782/IT/2024-4-4

SECURE DATA PROCESSING IN BUSINESS-INTERNET PLATFORMS AND E-COMMERCE SYSTEMS

Globalization and the development of the Internet have radically changed the ways in which information is exchanged and processed, becoming a destructive force in modern society. Every day, a huge amount of data is transmitted in various formats – text, audio, video, which contributes to progress in the economy, science, education and other areas. The Internet has become a universal platform for integrating businesses, scientific communities and citizens of the world, providing an unprecedented level of interaction and access to information.

However, the rapid spread of information technologies carries significant risks. In particular, the protection of sensitive user data, which can be stolen, lost privacy, or even used for manipulation, has become central in the field of information security. This not only threatens individual users, but also undermines trust in digital services as a whole, which hinders their further development.

***Purpose of the work.** Consideration of the experience and challenges of practical implementation of data residency standards in business platforms that have client-server architecture, which must meet modern requirements for the protection of e-commerce systems.*

***Research methodology.** Empirical and theoretical methods are used in the work.*

***Scientific novelty.** The main technical approaches to ensure compliance with the requirements for data residency in business-Internet platforms and e-commerce systems are analyzed, namely: geographical location of servers, encryption and tokenization, access restrictions, and proxy servers.*

The lack of uniform approaches to identifying sensitive data and mechanisms for protecting it creates situations where users' personal information becomes vulnerable. Solving these problems requires the creation and improvement of international standards for data protection regulation, which will take into account the peculiarities of the global digital environment and contribute to the harmonization of national legislations.

***Conclusions.** The article states that the issue of data residency remains one of the main technical and legal challenges of today for modern business and e-commerce systems, where the main stumbling block is the client-server architecture of modern web platforms and other applications of the same architecture that operate on the global network.*

***Key words:** e-commerce systems, Internet, data protection, data processing, information security, business Internet platform, cybersecurity.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасний етап розвитку інформаційного суспільства характеризується постійним збільшенням обсягів даних, що генеруються, передаються, обробляються та зберігаються в глобальній мережі Інтернет. Ця тенденція відкриває нові можливості для ефективного використання інформації в різних сферах, таких як наука, бізнес,

електронна комерція, освіта тощо. Проте, разом з цими можливостями з'являються серйозні загрози, пов'язані з витоком чутливих даних, несанкціонованим доступом та маніпуляцією інформацією. Зокрема, відсутність єдиних стандартів щодо визначення чутливих даних та методів їх захисту спричиняє ситуації, коли особиста інформація користувачів стає вразливою.

Електронна комерція – це придбання чи продаж товару за допомогою електронних носіїв, чи через мережу, подібну до Internet. Дане поняття може включати в себе замовлення, оплату та доставку товарів або послуг. Глобалізація цифрових технологій ускладнює застосування локальних законодавств щодо регулювання обробки даних. Географічна децентралізація сучасних клієнт-серверних додатків особливо в бізнес і державній сфері часто означає те, що серверна частина системи розташована в одній країні, а користувач – в іншій. Така структура створює правову колізію між законодавствами різних держав, що обмежує можливості ефективного захисту даних.

Ця проблема є не лише теоретичною, але й має суттєве практичне значення у бізнесі та електронній комерції – формування довіри клієнтів до цифрових сервісів залежить від здатності компаній забезпечувати конфіденційність їхніх даних.

Розв'язання цієї проблем вимагає створення та удосконалення міжнародних стандартів регулювання захисту даних, які будуть враховувати особливості глобального цифрового середовища та сприяти гармонізації національних законодавств.

Аналіз останніх досліджень і публікацій. Проблема відповідності архітектури інформаційних систем вимогам щодо місця зберігання даних (data residency) є однією з основних у сучасних дослідженнях безпеки даних та регуляторної відповідності. Деякі дослідження висвітлюють різні аспекти цієї проблеми, зокрема формування стандартів, технічних підходів та правових рішень.

Найчастіше представляють фреймворк для рекомендацій щодо архітектур, що відповідають вимогам місця зберігання даних. Дослідження зосереджено на автоматизації вибору архітектурних рішень, які враховують регіональні нормативні вимоги, але не розглядають питання децентралізованих клієнт-серверних систем.

Інколи робота фокусується на переміщенні та перерозподілі веб-сервісів для забезпечення відповідності вимогам щодо резиденції даних. У статті розглянуто алгоритмічні підходи до мінімізації витрат на релокацію сервісів. Однак у роботі недостатньо розкрито питання інтеграції з існуючими правовими нормами різних країн.

У дослідженнях (Кларк, Джейкоб, 2018; Стьопочкін, Новіков, 2022) пропонується сервісний підхід до вирішення проблеми місця зберігання даних у хмарі. Описуються методи шифрування та управління доступом, однак недостатньо висвітлено організаційні аспекти впровадження таких рішень у великих розподілених системах.

Автори аналізують виклики та можливості стандартизації питань щодо резиденції даних. У роботі наголошено на важливості створення міжнародних стандартів, які враховують як технічні, так і правові аспекти (Богом'я, Кочегаров, 2023; Богом'я, Черемісіна, Ярмолатій, Бараненко, 2024).

Мета статті. Розгляд досвіду і викликів практичного впровадження стандартів резиденції даних в бізнес платформах, які мають клієнт-серверну архітектуру, що мають відповідати сучасним вимогам захисту систем електронної комерції.

Виклад основного матеріалу дослідження. Для розкриття теми варто розділити відповідь га гранульовані підпункти: об'єкти захисту, середовище захисту, методика захисту, варіанти технічної реалізації

Об'єкти захисту. Перш за все, важливо визначити, що таке чутливі дані – це інформація, яка потребує підвищеного захисту через її особисту, конфіденційну чи стратегічну цінність. Несанкціонований доступ до таких даних може мати серйозні негативні наслідки для окремих осіб, організацій або навіть для держави. До основних категорій чутливих даних належать: персональні дані (PII), які поділяються на звичайні та особливо чутливі, фінансові дані, конфіденційна інформація бізнесу та дані, що стосуються національної безпеки.

Персональні дані – це інформація, яка ідентифікує або може ідентифікувати конкретну особу. Прикладами можуть бути ім'я, адреса, номер телефону, ідентифікаційний номер (номер паспорта або соціального страхування), дата народження тощо. До особливо чутливих персональних даних, як правило, відносять більш критичні особисті дані, які потребують ще більшого захисту тобто медичні дані (медичні записи, історія захворювань – PHI, Personal Health Information), біометричні дані (відбитки пальців, скани сітківки), раса, етнічна приналежність, політичні або релігійні переконання, а також дані про сексуальну орієнтацію і гендерну ідентичність. Фінансовими даними вважаються дані, пов'язані з фінансовими

операціями, які можуть бути використані для шахрайства або крадіжки: банківські рахунки, номери кредитних карток (PCI – Payment Car Information), Інформація про доходи або кредити тощо.

Конфіденційні бізнес-дані – це дані, що стосуються комерційної діяльності компаній і є важливими для бізнесу. Серед них розрізняють – інтелектуальна власність (патенти, авторські права), стратегії розвитку, фінансові плани, комерційні таємниці, інформація про клієнтів, постачальників і партнерів. Даними національної безпеки вважається інформація, яка може поставити під загрозу безпеку держави, якщо вона потрапить до рук ворогів або конкурентів. Захист таких даних вимагає використання надійних технічних, організаційних і правових методів, які мінімізують ризики витоку, несанкціонованого доступу або інших загроз для конфіденційності й безпеки.

Середовище захисту. Сьогодні бізнеси найчастіше використовують веб-платформи для організації своєї діяльності, оскільки вони є основою для багатьох підприємств, незалежно від їхнього розміру. До найпоширеніших типів таких платформ належать: для управління ресурсами підприємства (ERP – Enterprise Resource Planning), для управління IT-послугами (ITSM – Information Technology Service Management), а також для управління продажами і взаєминами з клієнтами (CRM – Customer Relationship Management).

З точки зору власника бізнесу, веб-платформа – це комплекс програмних і апаратних компонентів, які дозволяють співробітникам і клієнтам (користувачам) взаємодіяти з даними та бізнес-логікою через інтернет, зокрема за допомогою хмарних сховищ. Однак з погляду IT-фахівця або спеціаліста з кібербезпеки, веб-платформа – це додаток з класичною клієнт-серверною архітектурою, де сам додаток складається з двох частин, між якими здійснюється зв'язок через глобальну мережу, зазвичай інтернет.

Перша частина (клієнтська) являє собою звичайний браузер. Це зручно, адже в такому випадку немає необхідності кожен раз створювати нову клієнтську частину для кожного нового додатку – достатньо лише розробити HTML-інтерфейс. В цій частині користувач має можливість переглядати інформацію від сервера в текстовому, графічному та мультимедійному форматах а також своїми діями(наприклад пошук) відправляти додаткові запити на серверну частину чи то для отримання додаткових даних чи для зміни та збереження поточних. Усі дані які бачить чи слухає користувач, будуть видалені з оперативної пам'яті клієнтської частини одразу після переходу на інший сайт чи закриття браузера. Друга частина (серверна) призначення для обробки запитів від користувачів та перманентного збереження і обробки даних. Як правило серверна частина архітектури клієнт-сервер завжди потужніша і як наслідок – більша в розмірах та не володіє такою мобільністю як клієнтська частина, тому і рідше змінює свою локацію чи майже не змінює. Зі зростанням глобалізації і цифровізації, дані клієнтів можуть розміщуватися на серверах у різних країнах. І тут постає питання «резиденції даних» – де саме знаходяться ці дані – на якому сервері і наскільки безпечно вони зберігаються і чи відповідає це вимогам регуляторів.

Дотримання вимог до резиденції даних особливо актуальне для бізнесів, що обробляють персональні дані або конфіденційну інформацію.

Все більше і більше країн приймають нові закони про контроль резиденства даних. Серед таких – GDPR (Загальний регламент про захист даних Європейського Союзу), який обмежує експорт персональних даних за межі ЄС; PDPA – Закон про захист персональних даних різних країн; HIPAA (Health Insurance Portability and Accountability Act) – американський закон, що регулює конфіденційність та безпеку медичних даних.

Україна намагається не відставати від сучасних світових тенденцій. Закон «Про інформацію», «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо.

Резидентство даних розвивається і навіть стає пов'язане з питаннями національної безпеки та все частіше розглядається як торгова зброя і огляд іноземних інвестицій.

Такі норми встановлюють суворі вимоги до розташування та доступу до чутливих даних. Звісно у появи цих норм є природні і очевидні причини але має свої наслідки і вплив на технічну складову.

Методика захисту в питанні резиденції даних. Найбільшим фактором сьогодення, який створює технічні виклики є конфлікт стандартів та регуляцій – як вже було зазначено вище, різні країни мають різні вимоги до резиденції даних, що не лише ускладнює ведення бізнесу на міжнародному рівні де співпрацюють учасники різних країн на одній платформі але й інколи унеможливлює використання тих чи інших клієнт-серверних платформ.

Одні країни забороняють бачити дані за їх межами, інші – передавати дані, інші – зберігати

і т.д. Це призводить до необхідності максимальної гнучкості а отже до грануляції технічних операцій над даними.

Варіанти технічної реалізації резиденції. Існує кілька основних технічних підходів для забезпечення відповідності вимогам щодо резиденції даних в бізнес-інтернет платформах та системах електронної комерції. Ось деякі з найбільш поширених варіантів:

1. **Географічне розміщення серверів** – цей підхід передбачає розміщення дублікатів серверів веб-платформи в різних країнах, що дозволяє компаніям контролювати, де саме зберігаються дані користувачів. Перевагою є швидке вирішення питання, але серед недоліків – висока вартість і складність технічної підтримки та обслуговування в довгостроковій перспективі.

2. **Шифрування та токенізація** – шифрування даних при їх передачі допомагає мінімізувати ризики при збереженні або пересиланні інформації через міжнародні мережі. Цей метод часто використовується в комбінації з іншими підходами для посилення захисту.

3. **Обмеження доступу** – налаштування доступу до даних для співробітників залежно від їхньої ролі, місцезнаходження та необхідності працювати з конкретною інформацією. Це дозволяє додатково контролювати доступ до чутливих даних.

4. **Проксі-сервери** – ці сервери використовуються в сфері кіберзахисту для токенізації даних. Проксі-сервери можуть діяти як шлюзи, які токенізують чутливі дані перед їх передачею через мережу, зберігаючи оригінальні дані на локальному сервері в юрисдикції, де зберігання дозволено. Токенізація дозволяє передавати тільки зашифровані або частково зашифровані дані, що підвищує безпеку і допомагає відповідати вимогам регуляторів.

Висновки. В даній статті розглянуто досвід і виклики практичного впровадження стандартів резиденції даних в бізнес платформах які мають клієнт-серверну архітектуру, що відповідають сучасним вимогам захисту систем електронної комерції.

Стаття демонструє сучасні варіанти реалізації вимог і спроби уніфікувати будь-яку реалізацію резиденції даних. Та не дивлячись на те, що проблематика залишається відкритою до можливих нових рішень і на те, що сучасний бізнес готовий вкладати значні ресурси в питання резиденції даних, сама архітектура «клієнт-сервер» базується на фізичних реаліях і з'явилася як результат використання природної архітектури, що накладає свої обмеження, які неможливо обійти, що в свою чергу, створює сильну залежність та необхідність співпраці між світовим законодавством та інженерно-технічними реалізаціями.

ЛІТЕРАТУРА:

1. Framework for Recommending Data Residency Compliant Application Architecture. URL: https://ieeexplore.ieee.org/document/9712154 (дата звернення 09.10.2024).

2. Web Services Relocation and Reallocation for Data Residency Compliance. URL: https://ieeexplore.ieee.org/abstract/document/10181214 (дата звернення 09.10.2024).

3. The Impact of data residency on cloud computing. URL: https://ieeexplore.ieee.org/document/8418109 (дата звернення 09.10.2024).

4. Data residency as a service: a secure mechanism for storing data in the cloud. URL: https://www.inderscience.com/offers.php?id=100875 (дата звернення 09.10.2024).

5. Data Residency Challenges and Opportunities for Standardization. URL: https://www.inderscience.com/offers.php?id=100875 (дата звернення 09.10.2024).

6. Architecting for Compliance and Data Residency. URL: https://medium.com/salesforce-architects/architecting-for-compliance-and-data-residency-13e5d5d9a87f (дата звернення 09.10.2024)

7. Scale across borders: build a multi-region architecture while maintaining data residency. URL: https://community.aws/content/2dhVhtsciD5gVBlCKUlHoszrDzU/scale-beyond-borders (дата звернення 09.10.2024).

8. Managing Data Residency – concepts and theory. URL: https://blog.frankel.ch/data-residency/1/ (дата звернення 09.10.2024).

9. "How AI is transforming cybersecurity" by Gary Eastwood, " URL: https: / / www. Information – age. com/how-ai-is-transforming-cybersecurity-123478294/ (дата звернення 09.10.2024).

10. Кларк Дж., Джейкоб Дж. ШІ та кібербезпека: загрози та рішення. *Журнал кібербезпеки*, 2018. 4 (1), С. 1–14.

11. І. В. Стьопочкін, О. М. Новіков. Методи штучного інтелекту в кібербезпеці: навч. посіб. для здобувачів спец. 125 «Кібербезпека», 2022. 82 с.

12. Богом'я В. І., Кочегаров В. С. Кібербезпека в хмарних сервісах за допомогою застосування криптографічних методів. *Водний транспорт.* № 1 (37). 2023. С. 239–246. doi.org/10.33298/2226-8553.2023.1.37.27

13. Богом'я В. І., Черемісіна Л. О, Ярмолатій А. В, Бараненко О. О. Резиденція даних сучасних бізнес платформ, їх систем аутентифікації та особливості технічної реалізації в глобальній мережі internet. *Водний транспорт.* № 3 (41). 2024. С. 240–246.

REFERENCES:

1. Framework for Recommending Data Residency Compliant Application Architecture. Retrieved from: https://ieeexplore.ieee.org/document/9712154 (accessed 09.10.2024).

2. Web Services Relocation and Reallocation for Data Residency Compliance. Retrieved from: https://ieeexplore.ieee.org/abstract/document/10181214 (accessed 09.10.2024).

3. The Impact of Data Residency on Cloud Computing. Retrieved from: https://ieeexplore.ieee.org/document/8418109 (accessed 09.10.2024).

4. Data Residency as a Service: A Secure Mechanism for Storing Data in the Cloud. Retrieved from: https://www.inderscience.com/offers.php?id=100875 (accessed 09.10.2024).

5. Data Residency Challenges and Opportunities for Standardization. Retrieved from: https://www.inderscience.com/offers.php?id=100875 (accessed 09.10.2024).

6. Architecting for Compliance and Data Residency. Retrieved from: https://medium.com/salesforce-architects/architecting-for-compliance-and-data-residency-13e5d5d9a87f (accessed 09.10.2024).

7. Scale Across Borders: Build a Multi-Region Architecture While Maintaining Data Residency. Retrieved from: https://community.aws/content/2dhVhtsciD5gVBlCKUlHoszrDzU/scale-beyond-borders (accessed 09.10.2024).

8. Managing Data Residency – Concepts and Theory. Retrieved from: https://blog.frankel.ch/data-residency/1/ (accessed 09.10.2024).

9. "How AI is Transforming Cybersecurity" by Gary Eastwood. Retrieved from: https://www.information-age.com/how-ai-is-transforming-cybersecurity-123478294/ (accessed 09.10.2024)

10. Clark, J., Jacob, J. (2018). SHI ta kiberbezpeka: zahrozy ta rishennya. Zhurnal kiberbezpeky, 4 (1), 1–14.

11. Stiopochkina, I. V., Novikov, O. M. (2022). Metody shtuchnoho intelektu v kiberbezpetsi [Methods of artificial intelligence in cyber security]: navch. posib. dlya zdobuvachiv spets. 125 "Kiberbezpeka" / KPI im. Ihorya Sikors'koho; uklad.:. Kyiv: KPI im. Ihorya Sikors'koho, 82 [in Ukrainian].

12. Bohomyia, V. I., Kocheharov, V. S. (2023). Kiberbezpeka v khmarnykh servisasakh za dopomohoyu zastosuvannya kryptohrafichnykh metodiv [Cyber security in cloud services using cryptographic methods]. *Vodnyy transport.* 1(37), 239–246 [in Ukrainian].

13. Bohomya, V. I., Cheremisina, L. O., Yarmolatii, A. V., Baranenko, O. O. (2024). Rezydentsiya danykh suchasnykh biznes platform, yikh system autentyfikatsiyi ta osoblyvosti tekhichnoyi realizatsiyi v holovnii merezhi internet [Data Residence of Modern Business Platforms, Their Authentication Systems and Features of Technical Implementation in the Global Internet]. *Vodnyy transport.* 3 (41), 240–246 [in Ukrainian].