ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.056:004.42+681 doi.org/10.33298/2226-8553.2024.3.41.27

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

Глобалізація та розвиток мережі інтернет докорінно змінили способи обміну й обробки інформації, ставши рушійною силою сучасного суспільства. Щодня передається величезний обсяг даних у різних форматах — текст, аудіо, відео, що сприяє прогресу в економіці, науці, освіті й інших сферах. Інтернет перетворився на універсальну платформу для інтеграції бізнесів, наукових спільнот і громадян світу, забезпечуючи безпрецедентний рівень взаємодії та доступу до інформації.

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.

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.

В статті наведено, що питання резиденції даних залишається одним з головних технічних і юридичних викликів сьогодення для сучасного бізнесу, 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: глобалізація, мережа Інтернет, обмін інформацією, обробка даних, безпека інформації, чутливі дані, регулювання даних, конфіденційність, кібербезпека

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасний етап розвитку інформаційного суспільства супроводжується постійним зростанням обсягів даних, які генеруються, передаються, обробляються та зберігаються в глобальній мережі інтернет. Ця тенденція відкриває нові можливості для ефективного використання інформації в науці, бізнесі, освіті та інших сферах людської діяльності. Однак одночасно із цим виникають серйозні загрози, пов'язані з витоком чутливої інформації, несанкціонованим доступом та маніпуляцією даними. Зокрема, відсутність єдиних підходів до визначення чутливих даних і механізмів їх захисту створює ситуації, коли особиста інформація користувачів стає вразливою.

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 сфері науки – забезпечення захисту даних є основою для розвитку міжнародних досліджень і безпечного обміну результатами.

У бізнесі – формування довіри клієнтів до цифрових сервісів залежить від здатності компаній забезпечувати конфіденційність їхніх даних.

У суспільстві – гарантування прав громадян на недоторканність приватного життя є ключовим принципом демократичних цінностей.

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.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Проблематика відповідності архітектури інформаційних систем вимогам щодо місця зберігання даних (data residency) є однією з ключових у сучасних дослідженнях з безпеки даних та регуляторної відповідності. Низка робіт висвітлює різні аспекти цієї теми, зокрема, формування стандартів, технічних підходів та правових рішень.

У [1, 7,8] запропоновано фреймворк для рекомендації архітектур, що відповідають вимогам щодо місця розташування даних. Дослідження акцентує увагу на автоматизації вибору архітектурних рішень, які враховують регіональні нормативні вимоги, але залишає поза увагою питання децентралізованих клієнт-серверних систем.

Робота [2, 9] 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.

Стаття [3,10,11] аналізує вплив вимог щодо резиденції даних на використання хмарних технологій. Автори наголошують, що такі вимоги обмежують гнучкість використання хмарних сервісів, але залишають відкритими питання щодо розробки механізмів гармонізації міжнародних стандартів.

Дослідження [4, 12, 13] пропонує сервісний підхід до вирішення проблеми місця зберігання даних у хмарі. У статті описано методи шифрування та управління доступом, однак недостатньо висвітлено організаційні аспекти впровадження таких рішень у великих розподілених системах.

Звіт [5, 14] аналізує виклики та можливості стандартизації питань щодо резиденції даних. У роботі наголошено на важливості створення міжнародних стандартів, які враховують як технічні, так і правові аспекти.

Отже, попри значний прогрес у дослідженнях, залишаються невирішеними такі аспекти:

1. *Гармонізація національних законодавств*. Жодна з проаналізованих робіт не пропонує універсального підходу до узгодження регіональних законодавчих норм у глобальних клієнт-серверних системах.

2. *Моделі для децентралізованих архітектур*. Недостатньо уваги приділено питанням правового регулювання децентралізованих систем із географічно розподіленими компонентами.

3. *Практичне впровадження стандартів*. Існуючі дослідження не повною мірою розкривають організаційні та економічні аспекти реалізації запропонованих моделей у міжнародному середовищі.

Мета статті. Ця стаття спрямована на розгляд досвіду і викликів практичного впровадження стандартів резиденції даних в бізнес платформах і їх системах аутентифікації, які мають клієнт-серверну архітектуру, що мають відповідати сучасним вимогам захисту даних і їх резиденції.

Виклад основного матеріалу дослідження. Для розкриття теми «Технічні аспекти дотримання вимог стандартів і законів щодо безпечного розташування чутливих даних в глобальних мережах сучасних бізнес веб-систем», варто розділити відповідь га гранульовані підпункти: об'єкти захисту, середовище захисту, методика захисту, варіанти технічної реалізації

Об'єкти захисту. Перш за все розглянемо поняття чутливих даних - це дані, які потребують особливого захисту через їхню особисту, конфіденційну або стратегічну важливість.

Несанкціонований доступ до таких даних може призвести до негативних наслідків для осіб або організацій, або навіть держави. Можна виділити наступні категорії чутливих даних: персональні дані (PII) - звичайні і особливо чутливі, фінансові дані, конфіденційні бізнес дані та дані 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. Це можуть бути військові плани, державні таємниці, інформація про критичну інфраструктуру країни. 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. Бізнес сьогодні найчастіше використовує веб-платформи для організації своєї діяльності. Вони є основою для багатьох бізнесів, незалежно від їхнього масштабу. А серед найпоширеніших можна виділити такі типи - для управління підприємством (ERP - Enterprise Resource Planning), для управління IT-послугами (ITSM - Information Technology Service Management), для управління продажами і відносинами з клієнтами (CRM - Customer Relationship Management). З точки зору власника бізнесу, веб-платформа – це набір програмних і апаратних компонентів, що дозволяють співробітникам і клієнтам (користувачам) взаємодіяти з даними і бізнес-логікою через глобальну мережу інтернет, в тому числі використовуючи хмарні сховища. Але з точки зору айтівця або спеціаліста з кібербезпеки - веб-платформа це такий самий додаток як і інші, який має клієнт-серверну архітектуру. Тобто, сам додаток можна представити як систему з двох частин між якими працює глобальний канал комунікації - як правило інтернет (див. рис.1).

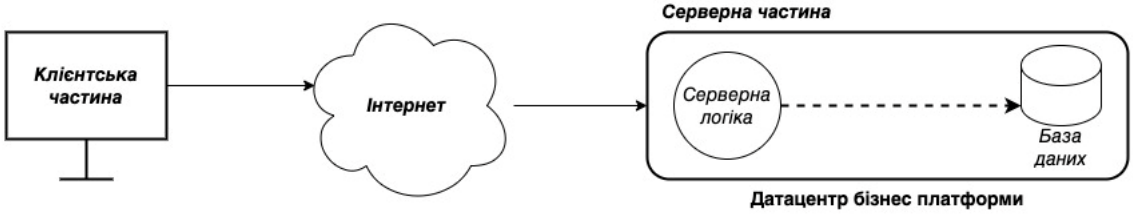

Рисунок 1 – Клієнт-серверна архітектура веб-платформи

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 та державних установ, що обробляють персональні дані або конфіденційну інформацію.

На сьогоднішній день у питанні захисту даних і їх резиденції прослідковуються такі тенденції.

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.

Китайські закони “Про захист персональної інформації”, “Про кібербезпеку”, “Про захист даних” також зобов'язують контролювати операції чутливою інформацією але є більш складними для розуміння.

Звісно ж і Україна намагається не відставати від сучасних світових тенденцій. Закон “Про інформацію”, “Про захист персональних даних”, “Про захист інформації в інформаційно-телекомунікаційних системах” тощо.

Резиденство 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. Така ситуація створює необхідність максимально гнучко підійти до забезпечення даних і це можливо лише роздробленням усіх операцій на атомарні - читання (перегляд) даних, збереження та обробка (зміна) даних (див рис.2).

Рисунок 2 – Атомарні операції з даними

Варіанти технічної реалізації резиденції. Існують декілька основних технічних підходів забезпечення відповідності вимогам резиденції даних і їх можна розділити на інженерно-організаційні, кібернетичні та комбіновані типи. Серед найпопулярніших визначають *Географічне розміщення серверів* – розміщення дублікатів серверної частини веб-платформи у різних країнах, що дозволяє компаніям контролювати, де зберігаються дані користувачів (див рис.3). Серед переваг такого підходу слід виділити критерій досить швидкого вирішення питання, але серед

відчутних недоліків - вартість та складна технічна підтримка і обслуговування в довгостроковій перспективі;

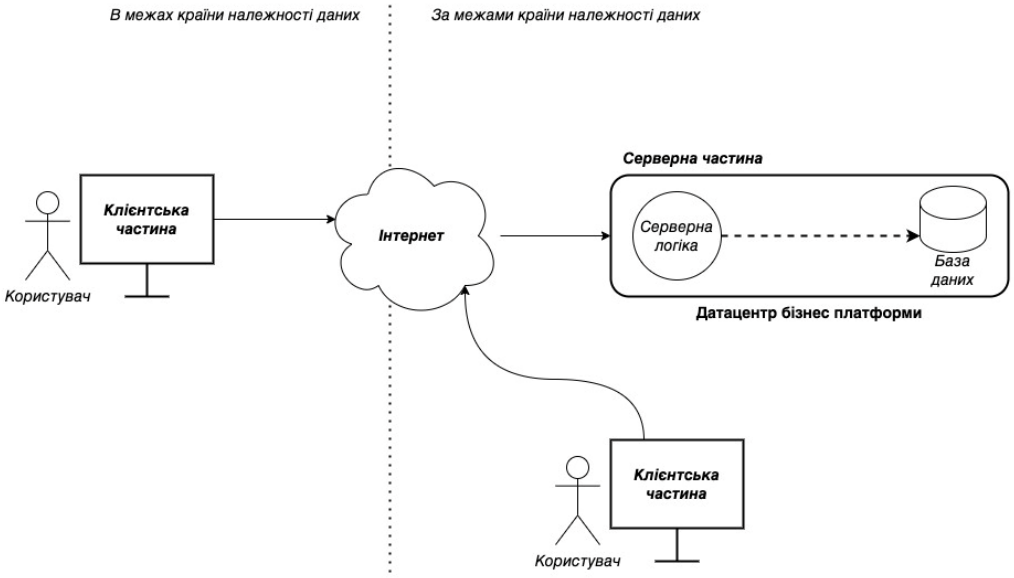

Рисунок 3 – Географічне регулювання резиденції даних

Шифрування та токенізація – передача зашифрованих даних мінімізує ризики при збереженні або пересиланні інформації через міжнародні мережі (див рис.4). Використовується в комбінації з іншими методами; *Обмеження доступу* – налаштування доступу для співробітників залежно від їх ролі та місцезнаходження і необхідності в роботі з конкретними даними.

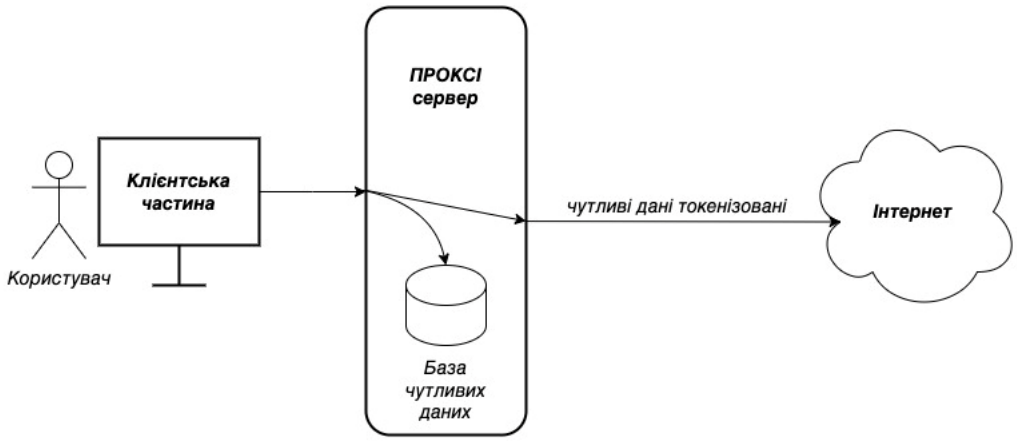

Рисунок 4 – Передача і токенізація даних через проксі сервер

Проксі-сервер (див рис.4) має дуже багато застосувань в сфері кіберзахисту, і в контексті резиденції чутливих даних використовується його функція токенізації даних - коли проксі-сервери працюють як шлюз, що токенізує чутливі дані перед їх відправкою через мережу, зберігаючи оригінальні дані на локальному сервері в юрисдикції, де зберігання дозволене. Токенізація допомагає передавати тільки зашифровані або частково зашифровані дані, що підвищує безпеку і допомагає відповідати вимогам регуляторів.

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

Стаття демонструє сучасні варіанти реалізації юридичних 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 (географічних) 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 [Електронний ресурс]. – Режим доступу: https://ieeexplore.ieee.org/document/9712154 (дата звернення 09.10.2024). – Назва з екрана
2. Web Services Relocation and Reallocation for Data Residency Compliance [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/abstract/document/10181214 (дата звернення 09.10.2024). – Назва з екрана
3. The Impact of data residency on cloud computing [Електронний ресурс]. – Режим доступу: https://ieeexplore.ieee.org/document/8418109 (дата звернення 09.10.2024). – Назва з екрана.
4. Data residency as a service: a secure mechanism for storing data in the cloud [Електронний ресурс]. – Режим доступу: https://www.inderscience.com/offers.php?id=100875 (дата звернення 09.10.2024). – Назва з екрана.
5. Data Residency Challenges and Opportunities for Standardization [Електронний ресурс]. – Режим доступу: https://www.inderscience.com/offers.php?id=100875 (дата звернення 09.10.2024). – Назва з екрана
6. Architecting for Compliance and Data Residency [Електронний ресурс]. – Режим доступу: https://medium.com/salesforce-architects/architecting-for-compliance-and-data-residency-13e5d5d9a87f (дата звернення 09.10.2024) - Назва з екрана.
7. Scale across borders: build a multi-region architecture while maintaining data residency [Електронний ресурс]. – Режим доступу: https://community.aws/content/2dhVhtsciD5gVBlCKUlHoszrDzU/scale-beyond-borders (дата звернення 09.10.2024) - Назва з екрана.
8. Managing Data Residency - concepts and theory [Електронний ресурс]. – Режим доступу: https://blog.frankel.ch/data-residency/1/ (дата звернення 09.10.2024) – Назва з екрана.
9. Understanding Architectures for Multi-Region Data Residency [Електронний ресурс]. – Режим доступу: https://www.infoq.com/articles/understanding-architectures-multiregion-data-residency/ (дата звернення 09.10.2024). – Назва з екрана.
10. Recommendations for using availability zones and regions [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/azure/well-architected/reliability/regions-availability-zones (дата звернення 09.10.2024). – Назва з екрана.
11. "How AI is transforming cybersecurity" by Gary Eastwood, " [Електронний ресурс]. Режим доступу до ресурсу: https: / / www. Information - age. com/how-ai-is-transforming-cybersecurity-123478294/ (дата звернення 09.10.2024). – Назва з екрана.
12. Кларк, Дж., Джейкоб, Дж. (2018). ШІ та кібербезпека: загрози та рішення. Журнал кібербезпеки, 4(1), С. 1-14.
13. І.В. Стьопочкін, О.М. Новіков. Методи штучного інтелекту в кібербезпеці: навч. посіб. для здобувачів спец. 125 «Кібербезпека», 2022. 82 с.
14. 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.

REFERENCE

1. Framework for Recommending Data Residency Compliant Application Architecture [Electronic resource]. – Access mode: https://ieeexplore.ieee.org/document/9712154 (accessed 09.10.2024). – Title from the screen.
2. Web Services Relocation and Reallocation for Data Residency Compliance [Electronic resource]. Access mode: https://ieeexplore.ieee.org/abstract/document/10181214 (accessed 09.10.2024). – Title from the screen.
3. The Impact of Data Residency on Cloud Computing [Electronic resource]. – Access mode: https://ieeexplore.ieee.org/document/8418109 (accessed 09.10.2024). – Title from the screen.
4. Data Residency as a Service: A Secure Mechanism for Storing Data in the Cloud [Electronic resource]. – Access mode: https://www.inderscience.com/offers.php?id=100875 (accessed 09.10.2024). – Title from the screen.
5. Data Residency Challenges and Opportunities for Standardization [Electronic resource]. – Access mode: https://www.inderscience.com/offers.php?id=100875 (accessed 09.10.2024). – Title from the screen.
6. Architecting for Compliance and Data Residency [Electronic resource]. – Access mode: https://medium.com/salesforce-architects/architecting-for-compliance-and-data-residency-13e5d5d9a87f (accessed 09.10.2024). – Title from the screen.
7. Scale Across Borders: Build a Multi-Region Architecture While Maintaining Data Residency [Electronic resource]. – Access mode: https://community.aws/content/2dhVhtsciD5gVBlCKUlHoszrDzU/scale-beyond-borders (accessed 09.10.2024). – Title from the screen.
8. Managing Data Residency - Concepts and Theory [Electronic resource]. – Access mode: https://blog.frankel.ch/data-residency/1/ (accessed 09.10.2024). – Title from the screen.
9. Understanding Architectures for Multi-Region Data Residency [Electronic resource]. – Access mode: https://www.infoq.com/articles/understanding-architectures-multiregion-data-residency/ (accessed 09.10.2024). – Title from the screen.
10. Recommendations for Using Availability Zones and Regions [Electronic resource]. – Access mode: https://learn.microsoft.com/en-us/azure/well-architected/reliability/regions-availability-zones (accessed 09.10.2024). – Title from the screen.
11. "How AI is Transforming Cybersecurity" by Gary Eastwood [Electronic resource]. Access mode: https://www.information-age.com/how-ai-is-transforming-cybersecurity-123478294/ (accessed 09.10.2024) – Title from the screen.
12. Clark, J., Jacob, J. (2018). SHI ta kiberbezpeka: zahrozy ta rishennya. Zhurnal kiberbezpeky, 4(1), pp. 1-14.
13. Metody shtuchnoho intelektu v kiberbezpetsi: navch. posib. dlya zdobuvachiv spets. 125 "Kiberbezpeka" / KPI im. Ihorya Sikors'koho; uklad.: I.V. Stiopochkina, O.M. Novikov. – Kyiv: KPI im. Ihorya Sikors'koho, 2022 – 82 p.
14. Bohomyia V.I., Kocheharov V.S. Kiberbezpeka v khmarnykh servisasakh za dopomohoyu zastosuvannya kryptohrafichnykh metodiv. Vodnyy transport. No. 1 (37). 2023. pp. 239–246. doi.org/10.33298/2226-8553.2023.1.37.27

Bogomya V. I., Cheremisina L. O., Yarmolatiy A. V., Baranenko O.V.

DATA RESIDENCY IN MODERN BUSINESS PLATFORMS: AUTHENTICATION SYSTEMS AND TECHNICAL IMPLEMENTATION IN GLOBAL NETWORKS

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 also carries significant risks. Also, the issue of protecting sensitive user data, which can be stolen, lose confidentiality or even used for manipulation, has become central in the field of information security. This threatens not only individual users, but also undermines trust in digital services as a whole, which hinders their further development.

The lack of unified approaches to defining sensitive data and mechanisms for its protection creates confidentiality when users' personal information becomes vulnerable.

Solving these problems requires the creation and improvement of international standards for data protection regulation, which will affect the features of the global digital environment and contribute to the harmonization of national legislation.

The article states that the issue of data residency remains one of the main technical and legal challenges of today for modern business, where the main link is the client-server architecture of the modern web platform itself and other applications of this architecture that operate in the global network.

Keywords: globalization, Internet, information exchange, data processing, information security, sensitive data, data regulation, confidentiality, cybersecurity