© Yalanetskyi V. Architectural Transformation of Personal Data Storage in E-Commerce // Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 46-51. © This is an open access article under the CC BY 4.0 International license.

DOI: 10.18372/2225-5036.32.21645

АРХІТЕКТУРНА ТРАНСФОРМАЦІЯ ЗБЕРІГАННЯ ПЕРСОНАЛЬНИХ ДАНИХ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ

Валерій Яланецький

НТУУ «Київський політехнічний інститут імені Ігоря Сікорського», Україна



ЯЛАНЕЦЬКИЙ Валерій Анатолійович
Рік та місце народження: 1978 рік, м. Київ, Україна.
Освіта: КПІ ім. Ігоря Сікорського, 2002 рік.
Посада: ст. викладач кафедри інформаційних систем та технологій з 2018 року.
Наукові інтереси: автоматизовані системи, штучний інтелект, блокчейн.
Публікації: більше 30 наукових публікацій, серед яких наукові статті, матеріали та тези доповідей на конференціях.
E-mail: yalanetskyi.valerii@edu.kpi.ua
Orcid: 0000-0001-6163-0258

Анотація. *У статті досліджено проблему кібербезпеки інформаційних систем електронної комерції в контексті атак на ланцюги постачання та компрометації підрядників. Показано, що централізована архітектура Web 2.0, яка передбачає зберігання персональних даних клієнтів у сервісній інфраструктурі, створює структурну вразливість і підвищує ризик масових витоків у разі зламу допоміжних компонентів. На прикладі інциденту, пов'язаного з підрядником електронного магазину нумізматичної продукції Національного банку України, обґрунтовано необхідність перегляду підходів до управління персональними даними. Запропоновано архітектурну модель, що базується на принципах самосуверенної цифрової ідентичності, селективного розкриття атрибутів і використанні тимчасових криптографічних токенів доступу. У цій моделі персональні дані зберігаються під контролем клієнта, а системи електронної комерції здійснюють перевірку їх валідності без централізованого накопичення. Показано, що перехід від зберігання даних до перевірки доказів дозволяє зменшити поверхню атаки та мінімізувати наслідки компрометації підрядників.*
Ключові слова: *кібербезпека, електронна комерція, атака на ланцюг постачання, самосуверенна ідентичність, селективне розкриття атрибутів.*

Вступ

Інформаційні системи електронної комерції (ІСЕК) функціонують у складних цифрових екосистемах, де персональні дані (ПД) клієнтів передаються між продавцями, платіжними сервісами та логістичними підрядниками. Така модель взаємодії істотно розширює поверхню кібератаки та створює умови для компрометації ПД навіть у випадку зламу другорядного учасника процесу. Централізоване накопичення ПД в базах даних (БД) формує системну вразливість: успішна кібератака на один компонент інфраструктури може призвести до масового витоку даних. Отже, проблема має не лише технічний, а архітектурний характер. ІСЕК упродовж останнього десятиліття перетворилися на один із ключових елементів цифрової економіки. Вони забезпечують повний цикл взаємодії між виробником, посередником і споживачем – від ідентифікації клієнта та обробки замовлення до здійснення платежу й логістики доставки. Водночас саме ця комплексність і міжорганізаційна інтегрованість роблять такі ІСЕК об'єктом підвищеної уваги з боку кіберзловмисників. Електронна комерція акумулює значні обсяги фінансових, поведінкових і ПД, що формує високий рівень привабливості для кібератак.

Кібербезпека в ІСЕК виходить за межі класичного захисту вебзастосунків або платіжної інфраструктури. Сучасні загрози охоплюють компрометацію облікових записів, фішингові кампанії, ін'єкційні кібератаки, втручання у логістичні ланцюги постачання, зловживання привілеями доступу, а також витоки даних через підрядників та зовнішні сервіси. Особливість цих ІСЕК полягає в тому, що вони функціонують у середовищі постійної взаємодії з третіми сторонами – платіжними провайдерами, логістичними операторами, маркетинговими платформами, хмарними сервісами. Кожен із таких елементів розширює поверхню кібератаки та ускладнює контроль над повним життєвим циклом даних.

Суттєвою проблемою традиційних ІСЕК є централізоване накопичення ПД клієнтів. Така модель передбачає зберігання повних профілів користувачів у БД торговельних платформ або їхніх підрядників. За умов компрометації такі БД стають джерелом масштабних витоків, що мають не лише технічні, а й правові та репутаційні наслідки. При цьому навіть високий рівень захисту основної інфраструктури не гарантує безпеки, якщо дані обробляються або зберігаються у менш захищених компонентах екосистеми.

На момент підготовки статті в засобах масової інформації опубліковано публічне повідомлення про вразливість підрядника Національного банку України, що обслуговував ІСЕК нумізматичної продукції [1]. Але оприлюднення технічного звіту про інцидент або присвоєного відповідного ідентифікатора ураження (Common Vulnerabilities and Exposures, CVE) не відбулося. Тому можна лише припустити наступні сценарії компрометації: вразливість вебзастосунку, SQL-ін'єкція, несанкціонований доступ через API, помилка автентифікації, застарілий CMS/плагін, компрометація облікових даних, фішинг співробітника підрядника, витік паролів й

автентифікаційних даних (кредeнціалів), кібератака викраденими кредeнціалами та незахищеність БД. Отже сучасні інциденти у сфері електронної комерції демонструють, що компрометація підрядників може мати не менші наслідки, ніж кібератаки на базові ІСЕК.

У зв'язку з цим сучасні підходи до кібербезпеки в електронній комерції дедалі більше орієнтуються не лише на посилення периметра та моніторинг інцидентів, а й на переосмислення архітектури управління даними. На перший план виходять принципи мінімізації даних, розмежування доступу, контролю згоди користувача та побудови систем, у яких ризик витоку зменшується не тільки за рахунок технічних засобів захисту, але й через зменшення обсягу збереженої чутливої інформації. У традиційній моделі електронної комерції продавець або підрядник зберігає повні профілі ПД клієнтів. Передача даних між суб'єктами відбувається з надмірним обсягом інформації, що часто перевищує функціональну необхідність. Рис. 1 демонструє типову централізовану архітектуру (модель Web 2.0), у якій ПД дублюються в кількох системах. Уразливість такої моделі полягає в тому, що кожен вузол екосистеми стає потенційною точкою масового витоку ПД.

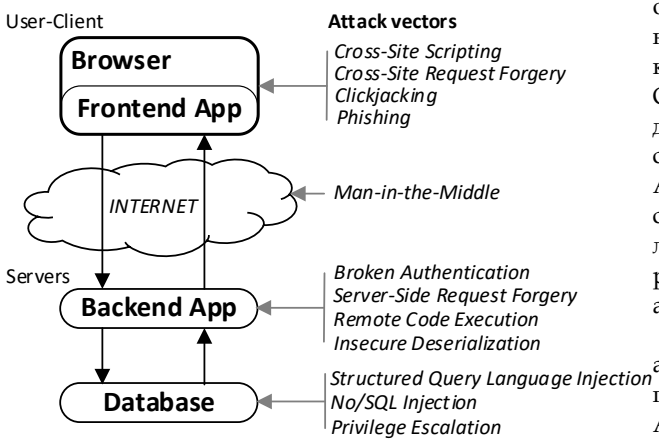


Рис. 1. Вразлива Web 2.0 модель зберігання ПД клієнта

У моделі Web 2.0 взаємодія клієнта з сервісом побудована навколо централізованої серверної інфраструктури. Клієнтський браузер і фронтенд-застосунок виконують роль інтерфейсу введення даних, через який користувач передає ПД – ідентифікаційні дані, контактну інформацію, адресу доставки. На цьому етапі виникає перша зона ризику, оскільки фронтенд часто залежить від сторонніх бібліотек, зовнішніх скриптів, систем аналітики або доставки контенту. Компрометація таких компонентів дозволяє перехоплювати введені ПД ще до їх передавання на сервер, що є типовим сценарієм кібератак на підрядників електронних сервісів.

Наступним критичним вузлом Web 2.0-архітектури є бекенд-застосунок підрядника. Саме тут відбувається обробка замовлень, інтеграція з платіжними та логістичними сервісами доставки, а також запис ПД до БД. У випадку помилок авторизації, уразливостей прикладного програмного інтерфейсу, компрометації облікових записів адміністраторів або недостатньо захищеної хмарної інфраструктури зловмисник отримує доступ до серверної логіки та може безпосередньо взаємодіяти з ПД клієнтів. Оскільки підрядник зазвичай має нижчий рівень кіберзахисту, ніж основна організація, саме цей компонент часто стає найслабшою ланкою ІСЕК.

Ключовою точкою ризику в моделі Web 2.0 є БД. У ній централізовано зберігаються повні профілі ПД клієнтів, включно з адресами доставки та контактною інформацією. Навіть якщо фінансові реквізити ізольовані або обробляються зовнішніми платіжними провайдерами, витік такої БД створює передумови для масового фішингу, соціальної інженерії та подальших цільових кібератак. Таким чином, сама архітектура Web 2.0 робить підрядника носієм високоризикового активу – централізованого сховища ПД.

Аналіз існуючих досліджень

Сучасні Web2-платформи електронної комерції та рітейлу характеризуються високим рівнем функціональної складності, широким використанням сторонніх сервісів, API, платіжних шлюзів і SaaS-компонентів, що суттєво розширює поверхню кібератаки. У зв'язку з цим упродовж останніх років спостерігається зростання кількості наукових досліджень, спрямованих на виявлення, класифікацію та аналіз вразливостей таких систем. Одним із найбільш репрезентативних сучасних досліджень є робота [2], у якій проведено систематичний аналіз безпеки популярних ІСЕК. Автори показують, що критичні вразливості Web2-e-commerce часто мають не лише технічний, а й логічний характер, зокрема пов'язані з некоректною реалізацією бізнес-процесів, управління ролями та авторизацією.

Дослідження [3] зосереджується на загальному аналізі вразливостей ІСЕК, підкреслюючи системну проблему недостатнього захисту ПД користувачів. Автори виокремлюють такі типові загрози, як SQL-ін'єкції, міжсайтові сценарні кібератаки (XSS), CSRF та фішингові механізми, що виникають через слабку валідацію введених даних і відсутність багаторівневого контролю доступу. Робота підтверджує, що навіть за наявності SSL/TLS базові помилки архітектури Web2-додатків залишаються основним джерелом компрометації. Автори роботи [4] доповнюють ці висновки практичним експериментальним аналізом реальних ІСЕК, демонструючи високу поширеність XSS-вразливостей, розкриття внутрішніх шляхів файлової системи та витоку чутливої інформації клієнтів. Автори наголошують, що значна частина таких проблем зумовлена використанням застарілих фреймворків і відсутністю регулярного аудиту безпеки.

У роботі [5] розглядаються сучасні тенденції розвитку вразливостей вебдодатків, зокрема у контексті мікросервісної архітектури та інтеграції сторонніх бібліотек. Показано, що у Web2-системах електронної комерції дедалі частіше з'являються складні комбіновані кібератаки, які поєднують

класичні уразливості (XSS, SQLi) з помилками конфігурації CI/CD-ланцюгів і хмарних сервісів. Окремий напрям сучасних досліджень стосується методів оцінювання та тестування безпеки. Зокрема, співавтори у [6] здійснили порівняльний аналіз інструментів сканування вразливостей вебдодатків, показавши, що жоден з автоматизованих сканерів не забезпечує повного покриття загроз Web2-e-commerce без поєднання з ручним аудитом. Автори [7] запропонували новий підхід, який дозволяє ефективніше виявляти ланцюжки кібератак, характерні саме для комерційних вебплатформ.

У відповідь на ці виклики розвиваються підходи селективного розкриття атрибутів ПД, які дозволяють підтверджувати необхідні властивості користувача без розкриття повного профілю [8]. Процесно-орієнтовані моделі такого розкриття спрямовані на запобігання кореляції дій користувача в різних контекстах [9]. Для логістичних сценаріїв пропонуються підходи щодо використання одноразових токенів і тимчасових атрибутів [10], а криптографічні механізми перевірюваних облікових даних дозволяють мінімізувати [11] передавання надлишкової інформації. Застосування цих підходів у міжорганізаційних процесах передбачає зберігання доказів подій замість самих ПД [12], а механізми відкликання цифрових облікових даних забезпечують контроль їхнього життєвого циклу [13]. Разом із тим дослідження вказують на виклики приватності [14] та систематизують проблеми впровадження *самосуверенної цифрової ідентичності* (*Self-Sovereign Identity*, SSI) в ICEK [15].

Інженерні аспекти децентралізованих ідентифікаторів безпосередньо впливають на стійкість архітектури до компрометації [16], що підтверджується узагальнюючими оглядами розвитку таких ICEK [17]. Алгоритмічні аспекти селективного розкриття атрибутів мають значення для масштабованості транзакцій [18], а інтеграція з розподіленими інфраструктурами дозволяє забезпечити довіру в складних цифрових середовищах [19]. Загальна тенденція до децентралізації цифрових сервісів підтверджує актуальність переосмислення [20] централізованих моделей управління даними.

Попри значну кількість досліджень, більшість з них зосереджується на окремих технічних аспектах SSI або селективного розкриття, тоді як питання інтеграції цих механізмів у повний бізнес-процес електронної комерції з урахуванням підрядників та логістики залишається недостатньо формалізованим.

Метою роботи є обгрунтування підходу до організації електронної комерції, у межах якого зберігання ПД замінюється зберіганням криптографічних доказів їхньої достовірності, що забезпечує персональний суверенітет користувача та зменшує наслідки можливих компрометацій. У межах цієї роботи науковий внесок полягає у формалізації прикладної архітектурної моделі електронної комерції, у якій ПД клієнтів повністю вилучені з ICEK продавця та його підрядників, а взаємодія між учасниками екосистеми здійснюється виключно на основі криптографічно перевірюваних доказів та тимчасових токенів доступу. Методологічною основою дослідження є аналіз реального інциденту компрометації підрядника, порівняльний аналіз архітектур Web 2.0 та Web 3.0 у контексті управління ПД, а також концептуальне моделювання архітектури зберігання криптографічних доказів замість зберігання самих ПД.

Основна частина дослідження

Централізована модель зберігання ПД у ICEK формує системну вразливість, підтверджену як практичними інцидентами, так і науковими дослідженнями. Виявлені в огляді обмеження існуючих підходів обумовлюють необхідність архітектурного рішення, яке дозволяє застосувати SSI та селективне розкриття ПД без модифікації базових бізнес-процесів електронної комерції, що і становить предмет подальшого розгляду.

Запропонована модель передбачає наявність у користувача персонального цифрового гаманця, підтримку перевірюваних облікових даних на стороні емітентів та базову готовність логістичних операторів до роботи з тимчасовими токенами доступу.

З урахуванням інциденту компрометації підрядника Національного банку України [1], пропонується перехід від Web 2.0 моделі централізованого зберігання ПД клієнтів до Web 3.0 моделі, заснованої на селективному розкритті атрибутів, SSI та використанні тимчасових токенів доступу. Основна ідея запропонованого рішення полягає у принциповому розділенні володіння ПД та їх використання в бізнес-процесах. ПД клієнта, зокрема ідентифікаційні дані, адреса доставки та контактна інформація, не зберігаються в ICEK або його підрядників, а залишаються під повним контролем клієнта у власному цифровому гаманці.

У запропонованій Web 3.0-моделі (рис. 2) центральним елементом стає клієнтський гаманець, у якому зберігаються ПД користувача. ПД більше не передаються у відкритому вигляді на сервер підрядника і не зберігаються у його БД. Децентралізований фронтенд-застосунок взаємодіє з гаманцем клієнта, а серверна частина (блокчейн мережа, децентралізований бекенд-застосунок та БД типу IPFS) виконує функцію перевірки доказів, а не обробки самих даних.

Отже, запропонований підхід полягає у переході від моделі накопичення ПД до моделі зберігання криптографічних доказів існування та володіння ПД. ПД залишаються у цифровому гаманці користувача, тоді як продавець і логістичний підрядник отримують лише перевірювані підтвердження необхідних атрибутів.

© Yalanetskyi V. Architectural Transformation of Personal Data Storage in E-Commerce // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 46-51. © This is an open access article under the CC BY 4.0 International license.*

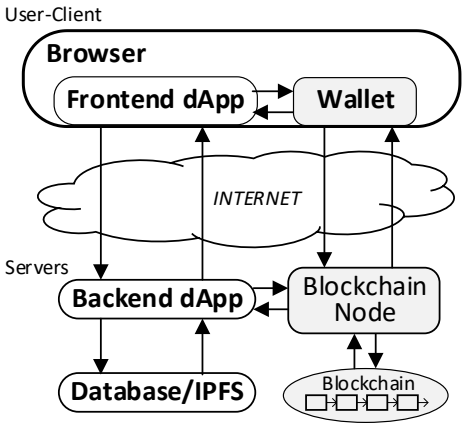


Рис. 2. Надійна Web 3.0 модель зберігання ПД клієнта

Архітектура децентралізованого зберігання ПД клієнта

У архітектурі Web 3.0 цифровий гаманець виступає не лише засобом зберігання криптографічних ключів або цифрових активів, а насамперед універсальною точкою входу (*end point*) користувача до децентралізованих додатків (dApps). Якщо в моделі Web 2.0 точкою входу є обліковий запис, що зберігається на сервері провайдера та керується через пару «*логін–пароль*», то у Web 3.0 SSI-ідентичність, авторизація і підпис дій зосереджені у клієнтському гаманці. Цифровий гаманець у цій моделі виконує функцію криптографічного інтерфейсу між користувачем і децентралізованою інфраструктурою. Він містить приватні ключі, які дозволяють підписувати транзакції, автентифікуватися у децентралізованих додатках і підтверджувати володіння певними цифровими атрибутами або токенами. Таким чином, гаманець стає персоналізованим криптографічним агентом користувача, через який здійснюється вся взаємодія з блокчейн-мережею або іншими розподіленими компонентами.

У контексті електронної комерції, гаманець може виконувати роль універсального засобу доступу до сервісу, інструменту підтвердження замовлення, механізму передачі тимчасових токенів доступу до атрибутів доставки та інтерфейсу взаємодії з логістичними або платіжними сервісами. Отже, у Web 3.0 цифровий гаманець є не просто сховищем активів, а ключовим архітектурним компонентом, який замінює традиційний серверний обліковий запис, зменшує залежність від централізованих баз даних і виступає єдиною криптографічною точкою входу користувача до екосистеми децентралізованих додатків.

У розширеній архітектурі Web 3.0 цифровий гаманець виконує не лише функцію криптографічного ключового сховища, а й роль контейнера перевірюваних ПД користувача, що випускаються довіреним емітентом. У такій моделі ПД не створюються самостійно користувачем і не зберігаються централізовано у сервісній інфраструктурі, а формуються у вигляді перевірюваних цифрових посвідчень, підписаних емітентом, який має відповідні повноваження. Емітентом може виступати державний орган, банк, акредитована установа або інший суб'єкт, який має право підтверджувати певні атрибути — наприклад, ім'я, дату народження, адресу проживання, податковий статус чи юридичну правосуб'єктність. Після ідентифікації особи емітент формує структурований цифровий документ, що містить набір атрибутів, метадані про строк дії та криптографічний підпис. Саме цей підпис забезпечує довіру до посвідчення та можливість його автоматичної перевірки будь-яким суб'єктом, який приймає такі документи.

Цифровий гаманець користувача зберігає такі посвідчення локально або у захищеному клієнтському середовищі. При цьому ключова відмінність від традиційних облікових записів полягає в тому, що гаманець не передає повний набір ПД під час кожної взаємодії. Замість цього він може формувати селективний доказ, який підтверджує лише необхідну властивість — наприклад, факт наявності чинної адреси або досягнення певного віку — без розкриття зайвої інформації. Таким чином, ПД залишаються під контролем користувача, а сервіс отримує лише підтвердження валідності конкретного атрибуту. Архітектурно це означає розподіл ролей: емітент відповідає за достовірність первинних даних, користувач — за їх зберігання та контроль розкриття, а сервіс — за перевірку криптографічної коректності доказу. Жоден із цих суб'єктів не володіє повним контролем над усім життєвим циклом ПД. Такий розподіл мінімізує ризик масових витоків, оскільки відсутнє централізоване сховище ПД, характерне для Web 2.0.

Отже, цифровий гаманець із перевірюваними ПД, виданими емітентом, формує нову модель довіри, у якій достовірність забезпечується криптографічним підписом, контроль — користувачем, а перевірка — сервісом. Такий підхід дозволяє поєднати вимоги безпеки, приватності та функціональності в умовах децентралізованої цифрової економіки. Рис. 3 ілюструє архітектуру, у якій у розподіленому реєстрі типу блокчейн фіксуються лише хеші та докази транзакцій, а не самі ПД. Навіть у випадку компрометації ICEK зловмисник не отримує доступу до повного профілю клієнта. Життєвий цикл цифрових ПД виглядає наступним чином.

Спочатку Емітент (*Issuer*) записує децентралізований ідентифікатор (Decentralized Identifier, DID) і набір відповідних атрибутів разом зі своїм відкритим цифровим ключем (та будь-яким іншим криптографічним матеріалом, необхідним для перевірки облікових даних емітента) у загальнодоступний (публічний або консорціумний) блокчейн за умови підтримки незмінності записів, публічної верифікації та довгострокової доступності DID-документів. Емітент використовує свій закритий цифровий ключ для цифрового підпису перевірених облікових даних, які він видає (поза блокчейном) кваліфікованому Власнику (*User/Holder*), а Власник зберігає їх у власному цифровому гаманці (*Wallet*). Верифікатор (*Verifier*) запитує у Власника цифрове підтвердження однієї або кількох облікових даних. Якщо Власник погоджується, гаманець Власника

© Yalanetskyi V. Architectural Transformation of Personal Data Storage in E-Commerce // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 46-51. © This is an open access article under the CC BY 4.0 International license.*

генерує та повертає підтвердження Верифікатору. Оскільки підтвердження містять DID емітента, Верифікатор використовує його для зчитування відкритого ключа Емітента та інших криптографічних даних з блокчейну. Наприкінці Верифікатор використовує відкритий ключ Емітента, щоб перевірити, чи є докази дійсними, а цифрові облікові дані не були підроблені.

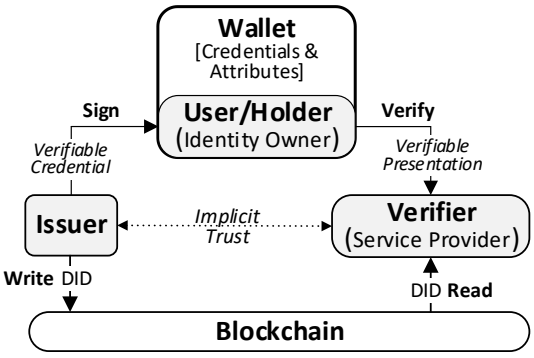


Рис. 3. Архітектура децентралізованого зберігання ПД клієнта

Отже у межах запропонованої моделі клієнт-власник володіє перевірюваними цифровими посвідченнями (креденціалами), що підтверджують валідність необхідних атрибутів, а ICEK взаємодіє з клієнтом не шляхом отримання та зберігання ПД, а шляхом перевірки криптографічних доказів їх існування та актуальності. Під час оформлення замовлення система отримує лише технічний ідентифікатор клієнта та доказ того, що необхідні атрибути, зокрема адреса доставки, є наявними і підтвердженими. Самі значення атрибутів при цьому не передаються і не зберігаються у БД підрядника.

Для реалізації фізичної доставки товарів пропонується механізм тимчасових токенів доступу (персональні атрибути клієнта). Після підтвердження замовлення формується запит на надання доступу до атрибуту доставки, який ініціюється ICEK, але реалізується безпосередньо на стороні клієнта. Клієнтський цифровий гаманець створює (випускає) одноразовий криптографічний токен, у якому зашифрована адреса доставки, і обмежує його використання конкретним логістичним оператором та визначеним часовим інтервалом. Такий токен передається безпосередньо перевізнику, який може отримати читабельну адресу лише в межах дозволеної операції та протягом строку дії токена. Після завершення доставки токен автоматично втрачає чинність (спалюється) і не може бути використаний повторно.

У запропонованій моделі ICEK та його підрядників оперують виключно внутрішніми ідентифікаторами замовлень, технічними маркерами та доказами виконання операцій. Жодна з цих сутностей не містить ПД у відкритому вигляді і не може бути використана для відновлення персонального профілю клієнта у разі компрометації ICEK. Контроль доступу до атрибутів і підзвітність учасників екосистеми забезпечуються через журнал подій доступу, в якому фіксуються факти створення та використання токенів, суб'єкти доступу та контекст операцій без зберігання самих ПД.

Таким чином, запропоноване рішення трансформує класичну модель «*збір і захист ПД*» у модель «*перевірка атрибутів ПД і контроль доступу*». Для ICEK нумізматичної продукції це означає радикальне зменшення обсягу довірених даних, усунення централізованих сховищ ПД у підрядників і суттєве зниження наслідків можливих кібератак на ланцюг постачання. Запропонований підхід узгоджується з сучасними науковими дослідженнями у сфері селективного розкриття атрибутів та SSI і може бути реалізований без порушення існуючих бізнес-процесів електронної комерції та логістики. У практичному сценарії фізичної доставки замовлення формується без передачі адреси продавцю або підряднику. ICEK фіксує лише ідентифікатор відправлення та доказ того, що адреса існує і підтверджена. Логістичний оператор ініціює запит на доступ до атрибуту доставки, після чого користувач надає селективне розкриття адреси конкретному перевізнику з обмеженням строку дії доступу. Після виконання доставки доступ автоматично припиняється. Продавець і його підрядники не володіють адресою у постійному вигляді, що принципово зменшує наслідки можливого зламу.

Маркування відправлення не містить ПД у відкритій формі. На бандеролі використовується технічний ідентифікатор або токен (наприклад, у вигляді QR-коду), який дозволяє авторизованій системі логістичного оператора отримати адресу через захищений цифровий канал лише в момент виконання операції. Для сторонніх осіб таке маркування не має інформативної цінності. Факти доступу, надання згоди та взаємодії учасників можуть фіксуватися у розподіленому журналі, що забезпечує незмінність аудиту без створення нового централізованого сховища ПД. Замість прямого передавання адреси або контактної інформації клієнт формує криптографічний доказ наявності та валідності відповідного атрибуту. Бекенд-застосунок підрядника перевіряє коректність такого доказу, не отримуючи доступу до змісту ПД. Це означає, що навіть у разі компрометації серверної інфраструктури зловмисник не зможе відновити персональні профілі клієнтів, оскільки ці дані фізично відсутні в системі.

Висновки

Запропоновано архітектуру, що дозволяє мінімізувати наслідки компрометації окремих компонентів екосистеми та забезпечити персональний суверенітет користувача в цифрових сервісах ICEK. У Web 3.0-моделі злам серверної частини не дає зловмиснику доступу до атрибутів ПД клієнтів, оскільки ICEK оперує лише технічними ідентифікаторами, доказами та тимчасовими токенами. Отже, застосування підходів SSI, селективного розкриття атрибутів і тимчасових

токенів не лише зменшує ймовірність успішної кібератаки, а й принципово змінює її наслідки, усуваючи саму можливість масового витоку ПД у підрядників електронної комерції. Запропонований підхід не усуває ризики повністю. До залишкових загроз належать компрометація цифрового гаманця користувача, помилки реалізації криптографічних механізмів та людський фактор у фізичному ланцюзі доставки. Проте такі інциденти матимуть локальний характер і не призводитимуть до масових витоків ПД.

Крім того, впровадження запропонованої моделі потребуватиме організаційної готовності учасників екосистеми, стандартизації форматів облікових даних та правового узгодження механізмів селективного розкриття ПД з чинним законодавством у сфері захисту ПД. Перехід від централізованого зберігання ПД до децентралізованого зберігання криптографічних доказів їх існування та контрольованого розкриття дозволяє суттєво зменшити ризики, пов'язані з кібератаками, зокрема на ланцюг постачання. Модель не замінює класичних механізмів кіберзахисту, але змінює саму економіку ризику, знижуючи привабливість ICEK як цілі для кібератак і обмежуючи масштаб потенційної шкоди.

Література

[1] Інтернет-магазин Нацбанку зазнав кібератаки, хакери могли отримати доступ до персональних даних [Електронний ресурс] // Укрінформ. – 2026. – 19 лютого. – Режим доступу: https://www.ukrinform.ua/rubric-economy/4093219-internetmagazin-nacbanku-zaznav-kiberataki-hakeri-mogli-otrimati-dostup-do-personalnih-danih.html.

[2] Pagey, R. All your shops are belong to us: Security weaknesses in e-commerce platforms / R. Pagey, M. Mannan, A. Youssef // Proceedings of the ACM Web Conference 2023 (WWW '23). – New York: Association for Computing Machinery, 2023. – DOI: https://doi.org/10.1145/3543507.3583319.

[3] Ray, S. Vulnerability and security analysis of e-commerce websites / S. Ray, R. Regunathan // Data Processing and Networking. – Cham: Springer, 2024. – DOI: https://doi.org/10.1007/978-981-96-5535-9_8.

[4] Baako, I. An integrated vulnerability assessment of electronic commerce websites / I. Baako, S. Umar // International Journal of Information Engineering and Electronic Business. – 2020. – Vol. 12, No. 5. – P. 23–34. – DOI: https://doi.org/10.5815/ijieeb.2020.05.03.

[5] Nawrocki, M. T. Vulnerabilities of web applications: Good practices and new trends / M. T. Nawrocki, J. Kołodziej // Applied Cybersecurity & Internet Governance. – 2024. – Vol. 3, No. 2. – P. 122–143. – DOI: https://doi.org/10.60097/ACIG/199521.

[6] Qadir, S. Comparative evaluation of web application vulnerability scanners / S. Qadir [et al.] // PeerJ Computer Science. – 2025. – DOI: https://doi.org/10.7717/peerj-cs.2821.

[7] Kaya, M. O. An effective new penetration test approach to detect web attacks on web applications / M. O. Kaya, H. A. Dagdogen, M. Ozdem, R. Das // Expert Systems with Applications. – 2025. – Vol. 241. – Art. 129623. – DOI: https://doi.org/10.1016/j.eswa.2025.129623.

[8] Bećirović Ramić, Š. Selective disclosure in digital credentials: A review / Š. Bećirović Ramić, E. Cogo, I. Prazina [et al.] // ICT Express. – 2024. – Vol. 10, No. 4. – P. 916–934. – DOI: https://doi.org/10.1016/j.icte.2024.05.011.

[9] Liu, J. Process-aware selective disclosure and identity unlinkability: A tag-based interoperability-enhancing digital identity framework / J. Liu, Z. Liang, Q. Lyu // Electronics. – 2026. – Vol. 15, No. 2. – Art. 473. – DOI: https://doi.org/10.3390/electronics15020473.

[10] Sun, N. A self-sovereign identity privacy-preserving scheme for logistics transportation based on one-time-use tokens / N. Sun, C. Zhu, Y. Liu // Electronics. – 2024. – Vol. 13, No. 14. – Art. 2799. – DOI: https://doi.org/10.3390/electronics13142799.

[11] Flamini, A. On cryptographic mechanisms for the selective disclosure of verifiable credentials / A. Flamini, G. Sciarretta, M. Scuro [et al.] // Journal of Information Security and Applications. – 2024. – Vol. 83. – Art. 103789. – DOI: https://doi.org/10.1016/j.jisa.2024.103789.

[12] Abid, A. A privacy-preserving traceability system for self-sovereign identity-based inter-organizational business processes / A. Abid, S. Cheikhrouhou, S. Kallel, M. Jmaiel // Computer Standards & Interfaces. – 2025. – Vol. 92. – Art. 103930. – DOI: https://doi.org/10.1016/j.csi.2024.103930.

[13] Fang, J. Privacy-enhanced distributed revocable identity management scheme based self-sovereign identity / J. Fang [et al.] // Journal of Cloud Computing. – 2024. – DOI: https://doi.org/10.1186/s13677-024-00715-8.

[14] Naicker, D. Challenges of user data privacy in self-sovereign identity verifiable credentials for autonomous building access during the COVID-19 pandemic / D. Naicker [et al.] // Frontiers in Blockchain. – 2024. – DOI: https://doi.org/10.3389/fbloc.2024.1374655.

[15] Satybaldy, A. A taxonomy of challenges for self-sovereign identity systems / A. Satybaldy, M. S. Ferdous, M. Nowostawski // IEEE Access. – 2024. – Vol. 12. – P. 16151–16177. – DOI: https://doi.org/10.1109/ACCESS.2024.3357940.

[16] Butincu, C. N. Design aspects of decentralized identifiers and self-sovereign identity systems / C. N. Butincu, A. Alexandrescu // IEEE Access. – 2024. – Vol. 12. – P. 60928–60942. – DOI: https://doi.org/10.1109/ACCESS.2024.3394537.

[17] Mazzocca, C. A survey on decentralized identifiers and verifiable credentials / C. Mazzocca, A. Acar, S. Uluagac [et al.] // IEEE Communications Surveys & Tutorials. – 2025. – DOI: https://doi.org/10.1109/COMST.2025.3543197.

[18]] Wang, G. An efficient distributed identity selective disclosure algorithm / G. Wang, G. Zhang // Applied Sciences. – 2025. – Vol. 15, No. 16. – Art. 8834. – DOI: https://doi.org/10.3390/app15168834.

[19] Ren, J. Blockchain-based self-sovereign identity management mechanism in AIoT environments / J. Ren, J. Zhang, Y. Ren, J. Xu // Electronics. – 2025. – Vol. 14, No. 19. – Art. 3954. – DOI: https://doi.org/10.3390/electronics14193954.

[20] Longshak, J. E. The emergence of Web3 and metaverse technologies: Implications for library and information services / J. E. Longshak // Global perspectives on sustainable library practices / ed. by V. Okojie, M. Igbinovia. – Hershey: IGI Global Scientific Publishing, 2023. – P. 84–113. – DOI: https://doi.org/10.4018/978-1-6684-5964-5.ch007.

УДК 004.738.5:339.138:004.056

Yalanetskyi V.A. Architectural Transformation of Personal Data Storage in E-Commerce

Abstract. *The article examines cybersecurity issues in e-commerce information systems in the context of supply chain attacks and contractor compromise. It is demonstrated that the centralized Web 2.0 architecture, which relies on storing customers' personal data within service infrastructures, creates structural vulnerabilities and increases the risk of large-scale data breaches when auxiliary components are compromised. Using the incident involving a contractor servicing the National Bank of Ukraine's numismatic online*

© Yalanetskyi V. Architectural Transformation of Personal Data Storage in E-Commerce // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 46-51. © This is an open access article under the CC BY 4.0 International license.*

store as an example, the need to reconsider approaches to personal data management is substantiated. An architectural model based on the principles of self-sovereign digital identity, selective attribute disclosure, and the use of temporary cryptographic access tokens is proposed. In this model, personal data remains under the control of the customer, while e-commerce systems verify the validity of attributes without centralized data accumulation. It is shown that the transition from data storage to proof verification reduces the attack surface and minimizes the consequences of contractor compromise.
Keywords: *cybersecurity, e-commerce, supply chain attack, self-sovereign identity, selective disclosure of attributes.*

Яланецький Валерій Анатолійович, ст. викладач кафедри інформаційних систем та технологій, Київський політехнічний інститут ім. Ігоря Сікорського,
Valerii Yalanetsyi, Senior Lecturer, Department of Information Systems and Technologies, Igor Sikorsky Kyiv Polytechnic Institute.

Дата надходження:	Дата прийняття:	Дата публікації:
28.02.2026	27.03.2026	22.04.2026