УДК 002.1:004:303.094.4](477+4):004.056
DOI: https://doi.org/10.31866/2617-796X.9.1.2026.362620

Марина Цілина,
кандидат філологічних наук, доцент,
доцент кафедри інформаційної діяльності
та зв'язків з громадськістю,
Київський національний університет
культури і мистецтв,
Київ, Україна
e-mail: macilin@ukr.net
https://orcid.org/0000-0001-5339-5147

ЕЛЕКТРОННА ІДЕНТИФІКАЦІЯ ТА ЦИФРОВА ДОКУМЕНТАЦІЯ: ЄВРОПЕЙСЬКИЙ ДОСВІД І ВИКЛИКИ КІБЕРБЕЗПЕКИ

Мета статті – зробити комплексний аналіз сучасних процесів цифровізації державного управління в Україні, зокрема у сфері електронної ідентифікації та цифрової документації, у контексті розвитку цифрового уряду, упровадження міжнародних стандартів eIDAS та інтеграції українських систем з європейськими практиками. Визначити роль електронної ідентифікації у забезпеченні доступності державних послуг, соціальної мобільності громадян та цифрової довіри. Оцінити основні ризики кібербезпеки, пов'язані з функціонуванням цифрових державних сервісів, та їх вплив на стабільність і безпеку суспільства. Проаналізувати перспективи подальшої інтеграції українських цифрових систем у європейський і глобальний цифровий простір.

Методи дослідження. Застосовано сукупність загальнонаукових методів: аналітичний метод – для узагальнення нормативно-правових актів та наукових джерел щодо електронної ідентифікації та цифрової документації; порівняльний метод – у ході зіставлення українського та європейського досвіду впровадження систем eID; системний підхід – під час розгляду цифровізації державного управління як багатовимірного процесу, що охоплює технологічні, правові та соціальні аспекти; оглядово-описовий метод – для фіксації сучасних практик, інцидентів і досліджень у сфері цифрової ідентифікації та державних електронних сервісів; структурно-функціональний аналіз – для визначення ключових інструментів, ризиків і викликів кібербезпеки в цифровій державній екосистемі.

Наукова новизна. Стаття є системним оглядом сучасних практик електронної ідентифікації та цифрової документації в Україні, поєднує аналіз державних стратегій, нормативно-правових актів, міжнародних стандартів eIDAS та європейських практик цифрового урядування, що дає змогу визначити ключові виклики, ризики кібербезпеки й перспективи інтеграції українських цифрових систем у європейський та глобальний цифровий простір.

Висновки. Цифрова трансформація державного управління підкреслює роль електронної ідентифікації та цифрової документації як фундаменту цифрового суспільства, забезпечуючи підтвердження особи, правомірність документообігу та довіру між громадянами, державою і бізнесом. Досвід ЄС показав, що ефективні системи залежать від цифрової інфраструктури, нормативно-правової гармонізації та цифрової грамотності населення, а приклад Естонії підтверджує потенціал eID для розвитку цифрової держав-

ності. В Україні платформа «Дія», BankID НБУ та кваліфіковані підписи формують довіру до цифрових сервісів і поступово інтегруються з європейськими стандартами, але зберігаються ризики: централізація реєстрів, можливість витоку даних, соціальний інжиніринг, залежність від IT-інфраструктури та вразливості програмного забезпечення, що особливо критично в умовах війни.

Цілком можливо, що протягом наступних 3–5 років масштабне впровадження мобільних рішень eID та інтеграція з European Digital Identity Wallet підвищать цифрову доступність державних сервісів, а розвиток кіберзахисту й цифрової грамотності населення мінімізує ризики витоку даних і шахрайства. За умови гармонізації українських стандартів із європейськими та розвитку резервної інфраструктури понад 80 % громадян зможуть користуватися електронними державними сервісами до 2030 року, що сприятиме формуванню стабільної цифрової довіри.

Отже, подальший розвиток eID в Україні потребує одночасного посилення нормативного регулювання, кіберзахисту, резервування IT-інфраструктури та інтеграції з європейськими стандартами, що забезпечить надійність цифрових сервісів і підвищить цифрову стійкість держави.

Ключові слова: електронна ідентифікація; цифрові документи; BankID; кібербезпека; цифрова нерівність; державні сервіси; цифровий суверенітет.

Вступ. У XXI столітті суспільство зазнає трансформації, що визначається поширенням цифрових технологій і консолідацією інформаційних ресурсів як ключового чинника соціально-економічного розвитку. Ці зміни зумовлюють технічні, соціальні, правові й політичні зрушення. З огляду на це актуальним стає дослідження електронної ідентифікації та цифрової документації, що формують простір цифрової довіри, яка є основою взаємодії громадянин – держава – бізнес у цифровому суспільстві. Цифрова ідентифікація набуває особливого значення в умовах війни: фізичні канали взаємодії громадян із державою часто порушуються, а електронні сервіси стають єдиним доступним каналом отримання соціальних послуг, реєстрації прав і здійснення адміністративних процедур. В Україні, наприклад, у воєнний період електронна ідентифікація стала критичною для отримання допомоги ВПО, доступу до медичних послуг у евакуації та отримання соціальних виплат без фізичної присутності.

У міжнародній науковій спільноті питання цифрової ідентичності розглядають через призму інформаційного суспільства та цифрової довіри. Теоретичні засади такого підходу сформовано у працях дослідників інформаційного суспільства, які ще на початку розвитку цифрової епохи звернули увагу на зміну ролі інформації, мереж та ідентичності в соціальних і політичних процесах. Зокрема, М. Кастелс (Castells, 2010) у фундаментальному дослідженні «Становлення мережевого суспільства» («The rise of the network society») розглядає механізми цифрової взаємодії як структуру, що формує мережеву державу та мережеву економіку, де інформація ідентичності стає ресурсом влади й участі в суспільному житті. Д. Берч (Birch, 2014) у книзі «Ідентичність – це нові гроші» («Identity is the new money») пояснює, що цифрова ідентичність стає інструментом доступу до сервісів й економічним активом, що має цінність у цифровій економіці. У нормативно-правових актах міжнародних організацій, зокрема Організації економічного співробіт-

ISSN 2617-796X (print)
ISSN 2618-0049 (online)

ництва та розвитку і Європейської комісії, розглянуто вплив стандартизації eID на транскордонну мобільність, цифрову інклюзію та розвиток єдиного цифрового ринку (Regulation (EU) No 910/2014 of the European Parliament and of the Council, 2014). Ці дослідження підкреслюють, що електронну ідентифікацію не можна розглядати суто як технічну функцію. Це структурний елемент цифрової екосистеми, що впливає на економічні та соціальні процеси.

У сучасній Україні розвиток електронної ідентифікації та цифрової документації досліджують з різних аспектів. М. Вовк, О. Заяць, Ю. Юркевич (Vovk, Zaiats and Yurkevych, 2024) розглядають правові аспекти eID та електронних довірчих послуг, їх узгодження з європейським законодавством і перспективи вдосконалення регуляторної бази. Вони підкреслюють, що ефективна електронна ідентифікація потребує правової гармонізації з міжнародними стандартами, а також чіткого визначення юридичного статусу цифрових ідентифікаційних засобів.

М. Ковалів, І. Красницький, С. Пєтко, С. Єсімов, В. Корецька, О. Явний (2024) аналізують нормативно-правові акти України та ЄС щодо електронної ідентифікації. Автори вказують, що правова база eID є системотворчою для розвитку цифрових державних сервісів, оскільки вона визначає порядок встановлення особи та права й обов'язки учасників інформаційних відносин, що підвищує довіру до цифрових сервісів та інформаційну безпеку.

Ю. Худолій, В. Дорош (2025) розкривають технічні й організаційні аспекти застосування eID та цифрового підпису у фінансових установах. Вони акцентують увагу на ризиках та механізмах кіберзахисту, що дає змогу зрозуміти практичну реалізацію цифрових ідентифікаційних систем і оцінити загрози в конкретному секторі економіки.

Попри значну кількість досліджень, присвячених теоретичним, правовим і технічним аспектам електронної ідентифікації, у науковій літературі все ще недостатньо комплексно розкрито взаємозв'язок між розвитком цифрової ідентифікації, цифрової документації та процесами цифровізації державного управління в Україні в контексті інтеграції до європейського цифрового простору. Також потребують подальшого аналізу питання впливу електронної ідентифікації на доступність державних послуг, формування цифрової довіри та ризики кібербезпеки, пов'язані з функціонуванням цифрових державних сервісів.

З огляду на це необхідно провести комплексний аналіз сучасних процесів цифровізації державного управління в Україні, зокрема у сфері електронної ідентифікації та цифрової документації, у контексті розвитку цифрового уряду, впровадження міжнародних стандартів eIDAS та інтеграції українських систем із європейськими цифровими практиками.

Результати дослідження. Електронна ідентифікація (eID) забезпечує підтвердження особи у цифровому середовищі за допомогою юридичних і технічних засобів. Вона є фундаментом довіри між громадянами, бізнесом і державою, забезпечуючи безпечний обіг інформації та легалізацію електронних документів.

В Україні розвиток eID здійснюється через платформу «Дія», BankID НБУ та кваліфіковані електронні підписи. Законодавча база представлена Законом Украї-

їни «Про електронну ідентифікацію та електронні довірчі послуги» (Верховна Рада України, 2022), який гармонізований з регламентом ЄС eIDAS.

У цілому електронна ідентифікація формує технічну основу цифрової державності, є соціальним та економічним інструментом для прискорення обслуговування громадян. Для повного розуміння ефективності необхідно оцінити українську модель у контексті європейських практик.

У ЄС цифрова ідентифікація реалізована на національному рівні, проте моделі та масштаби використання значно відрізняються. Б. Батке (2025), цитуючи Ільвіса, автора дослідження «Кінець бюрократії», зазначає, що в Естонії національним цифровим ID для доступу до держпослуг користується 90 % громадян, у Німеччині – менш ніж 10 %. А Бельгія ще декілька років тому використовувала технологію е-ідентифікаторів, схожу на німецьку. Однак вона працювала погано, і тільки 10–20 % населення нею користувалося. Проте, коли банки й телеком-оператори запровадили зручну мобільну версію, що дала змогу отримувати доступ як до приватних, так і до державних сервісів, кількість користувачів eID зросла до 80 %.

Загальноєвропейська статистика також підтверджує значні відмінності у рівні використання цифрових державних сервісів. За даними індексу цифрової економіки та суспільства (DESI), у 2024 р. 70 % людей віком 16–74 років у ЄС заявили, що вони користувалися вебсайтом або застосунком державного органу протягом попередніх 12 місяців. Серед країн Європейського Союзу Данія (98,5 %), Нідерланди (96,0 %) та Фінляндія (95,4 %) мали найвищу частку використання електронного урядування у 2024 році. Натомість Румунія (25,3 %), Болгарія (31,5 %) та Італія (55,1 %) мали найнижчі частки (70% of EU citizens used online public services in 2024, 2025).

Європейські практики демонструють, що масштабне впровадження eID потребує одночасно технологічної готовності, правової бази та високої цифрової грамотності громадян. Українська модель відзначається швидким зростанням користувачів і поступовою гармонізацією з eIDAS та Digital Identity Wallet.

Станом на 2025 р. платформа «Дія» налічує понад 23 млн користувачів (Держава без черг і паперів, 2025), а BankID НБУ забезпечив 109,4 млн успішних ідентифікацій (Жолобецький, 2026). Динаміка показує експоненційне зростання довіри до цифрових механізмів ідентифікації та трансформацію поведінкових моделей громадян. Такі показники дають змогу оцінити потенціал інтеграції українських цифрових систем у європейський контекст.

Електронна ідентифікація сприяє соціальній мобільності, особливо для внутрішньо переміщених осіб, забезпечуючи дистанційний доступ до медичних, освітніх і фінансових послуг.

Економічно цифровізація зменшує транзакційні витрати та пришвидшує обіг документів. Наприклад, реєстрація підприємства через «Дію» скорочується на 30–50 % часу порівняно з паперовими процедурами. У ЄС цифрові документи також оптимізують адміністративні процеси в публічному секторі.

Проте розвиток eID неможливий без оцінки ризиків, що виникають у кіберпросторі, особливо в умовах воєнного стану. Тому доцільно перейти до аналізу безпеки та загроз.

ISSN 2617-796X (print)
ISSN 2618-0049 (online)

За даними Європейського агентства з кібербезпеки (ENISA), сектор державного управління є найбільшою мішенню для кібератак у ЄС: на нього припадає близько 38 % усіх зафіксованих інцидентів, у цифровій інфраструктурі та послугах – 4,8 %, що поступилися галузі транспорту (7,5 %) і перевищили сферу фінансів (4,5 %) (EU consistently targeted by diverse yet convergent threat groups, 2025).

Ці дані підкреслюють високий рівень ризику централізованих державних систем, адже атаки на ключові сервіси можуть призвести до значних втрат даних.

Основні ризики охоплюють:

1. Централізацію реєстрів та баз даних. У разі збоїв чи атак на центральний сервер втрачається доступ до всіх електронних сервісів. Можливий одночасний витік великої кількості персональних даних користувачів, включно з паспортними даними, адресами, медичною інформацією та фінансовими реквізитами.

У січні 2026 року Європейська комісія повідомила, що її IT-системи для управління мобільними пристроями були атаковані і зловмисники могли отримати доступ до персональної інформації частини співробітників (імена, номери телефонів). Ситуація була локалізована протягом 9 годин, але інцидент підтвердив актуальність загроз для центральних цифрових інфраструктур ЄС (Arghire, 2026).

Моніторинг RIA (Estonian Information System Authority) фіксував у Естонії 852–1057 кібератак протягом окремих періодів 2025 року, включно з DDoS-атаками на офіційні е-послуги, виборчі ресурси й інші державні сервіси.

Наприклад, у жовтні 2025 р. було 1057 інцидентів (частина –denial-of-service атаки на сайти державних сервісів, включно з eesti.ee) (Situation in cyberspace – October 2025, 2026). Загалом прямої публічної документації про успішні кіберзломи конкретно електронних ідентифікаційних систем eID у ЄС у 2022–2026 рр. у відкритих джерелах не знайдено. Проте наведені масштабні атаки на державну цифрову інфраструктуру та ЄС-сервіси показують, що кіберзагрози реальні та впливають на суміжні сервіси, що посилює ризики централізації та доступу до цифрових ідентифікацій.

2. Витік персональних даних через слабкі паролі, неперевірені інтеграції або експлуатацію вразливостей. В Україні під час війни сформувався підвищений ризик незаконного збору даних про ВПО або держслужбовців через фішинг чи соціальні інженерні атаки.

У грудні 2024 р. російські хакери здійснили масштабну кібератаку на мережеву інфраструктуру Міністерства юстиції України, що обслуговує ключові державні реєстри. За оцінками експертів, унаслідок атаки зловмисники могли отримати частину критичних даних або доступ до інформаційних систем, що містять персональні відомості громадян.

Хоча офіційні органи повідомили, що витік персональних даних не підтверджено, сам інцидент показав уразливість централізованих державних реєстрів та потенційний ризик доступу до персональної інформації громадян. Атака могла поставити під загрозу дані державних реєстрів (реєстр актів цивільного стану, реєстр юридичних осіб, реєстр прав на нерухомість), які містять великі масиви персональної інформації (Мирончук, 2024).

У 2025 р. хакери атакували цифрові системи Legal Aid Agency, що належить Міністерству юстиції Великої Британії. Унаслідок атаки було викрадено значні обсяги персональної інформації заявників: імена, контактні дані, дати народження, номери соціального страхування, фінансову інформацію та інші чутливі дані (Davies, 2025).

У 2026 р. хакери отримали доступ до французької державної бази FICOBA, яка містить інформацію про банківські рахунки громадян. Злам став можливим через компрометацію облікового запису одного державного службовця. У результаті було розкрито дані приблизно 1,2 млн банківських рахунків, включно з іменами, адресами, IBAN-рахунками та податковими ідентифікаторами (Pala, 2026).

Наведені інциденти демонструють, що навіть розвинені державні цифрові системи залишаються вразливими до кібератак, фішингу та компрометації облікових записів. Це підтверджує те, що централізовані державні реєстри й інформаційні бази можуть становити значний ризик масового витоку персональних даних, що у свою чергу створює загрозу фінансового шахрайства, викрадення особистості й інших форм кіберзлочинності.

3. Ризик соціального інжинірингу та фішингових атак. Значна частина кіберінцидентів пов'язана не тільки з технічними вразливостями систем, а й з маніпуляціями людським фактором, що реалізується через методи соціального інжинірингу та фішингу.

Зловмисники можуть імітувати повідомлення від застосунку «Дія», банків або державних служб для отримання доступу до облікових записів. В умовах війни кількість таких атак зростає через психологічний тиск на громадян та спроби маніпулювати страхом і терміновістю. Прикладом таких дій слугує розсилання фальшивих електронних листів із запитом підтвердити BankID для отримання соціальної допомоги.

4. Залежність від IT-інфраструктури та відновлюваність. Збої в електропостачанні, інтернет-з'єднанні або серверних системах можуть повністю паралізувати доступ до eID-сервісів. В умовах війни резервування серверів та дата-центрів є критично важливим для безперервності роботи. У квітні 2025 р. в Україні стався масштабний збій у роботі низки цифрових сервісів, зокрема застосунку «Дія», банківських сервісів і логістичних платформ. Причиною стала технічна проблема в одному з дата-центрів, де розміщувалася інфраструктура цих систем. Унаслідок інциденту тимчасово не працювали електронні сервіси банків, платіжні системи та деякі державні цифрові послуги, що показало залежність цифрової екосистеми від стабільної роботи серверної інфраструктури (Опанасенко, 2025).

Під час російських атак на енергетичну інфраструктуру України у 2022–2024 рр. відключення електроенергії часто спричиняли перевантаження мобільних мереж та втрату доступу до інтернету, що ускладнювало використання цифрових сервісів і державних електронних систем.

У квітні 2025 р. великий збій у європейській енергосистемі призвів до масового відключення електроенергії для десятків мільйонів людей в Іспанії та Португалії, що спричинило зупинку транспортних систем, перебої мобільного зв'язку, інтернету, банківських операцій та електронних сервісів (Henley, Kassam and Jones, 2025).

Наведені приклади свідчать, що функціонування систем електронної ідентифікації та цифрових державних сервісів значною мірою залежить від стабільності

ISSN 2617-796X (print)
ISSN 2618-0049 (online)

ІТ-інфраструктури, енергопостачання та мережевого доступу. Тому забезпечення резервування серверів, дата-центрів і каналів зв'язку є критично важливим для гарантування безперервності роботи електронних сервісів і захисту доступу громадян до цифрових державних послуг.

5. Вразливості програмного забезпечення. Служба безпеки України разом з Офісом Генерального прокурора викрила організовану злочинну групу, яка несанкціоновано отримувала доступ до банківських акаунтів громадян та входила в застосунок «Дія» через систему авторизації BankID, використовуючи дані з онлайн-банкінгу (логіни, паролі та коди підтвердження). Це давало змогу зловмисникам здійснювати дії від імені потерпілих, включно з доступом до державних сервісів. Такий інцидент показує, що недостатньо захищені облікові дані третіх сторін (наприклад, онлайн-банку) можуть стати «входом» до державних сервісів через BankID, навіть якщо уразливість безпосередньо в системі BankID відсутня. Це підкреслює важливість комплексної безпеки: не лише платформ ідентифікації, але й суміжних сервісів, що на них спираються (Міністерство цифрової трансформації України, 2025).

У 2024 р. зафіксовано ситуацію, коли шахраї зламали облікові дані BankID львів'янки й отримали доступ до її облікового запису в «Дії», після чого оформили кредити на її ім'я (Прилуцький, 2024). Цей приклад демонструє, що компрометація облікового запису BankID на рівні мобільних застосунків або банку може призвести не тільки до втрати контролю над державними сервісами, а й до фінансових наслідків для користувача – оформлення кредитів або транзакцій без згоди власника.

Хоча конкретних випадків успішних масових атак на кваліфіковані електронні підписи у відкритих джерелах для 2022–2026 рр. не зафіксовано, експертні джерела та вимоги eIDAS підкреслюють, що безпека таких сертифікатів залежить від захищеності приватних ключів та сертифікаційних центрів. Кваліфіковані сертифікати підпису мають найвищий рівень довіри в цифровому середовищі, але їх компрометація (наприклад, витік приватного ключа або доступ до систем генерації підписів) може дозволити фальсифікацію документів і позбавити їх юридичної сили. Навіть якщо конкретних масштабних інцидентів немає у відкритих новинах, сама природа криптографічної інфраструктури означає, що слабкість у захисті приватних ключів, некоректна реалізація API чи віддалений доступ до генераторів підписів можуть бути використані зловмисниками, що загрожує юридичній недійсності документації, втраті довіри до електронних контрактів, шахрайству та матеріальним збиткам. Це підтверджено вимогами та рекомендаціями щодо безпеки eIDAS, які визначають суворі умови для довірчих послуг та управління сертифікатами.

6. Кіберзлочинність. Спеціально організовані кібератаки можуть паралізувати роботу держструктур або використовувати дані для стратегічної шкоди. В умовах воєнного стану ці ризики стають критичними для національної безпеки та соціальної стабільності.

Під час повномасштабного вторгнення Росії в Україну з 24 лютого 2022 р. були численні цілеспрямовані кібератаки на енергетичні об'єкти України. Хакери намагалися перешкодити управлінню електростанціями, вводили в експлуатацію шкідливі програми проти енергетичних систем і здійснювали DDoS-атаки на критичні сервіси,

що ускладнювало координацію робіт і резервування мереж. Через це було тимчасово порушено електропостачання в низці регіонів, що призвело до збоїв у роботі мобільного зв'язку, доступу до інтернету та онлайн-послуг, включно з державними. Кібератаки супротивника були спрямовані не тільки на цифрову інфраструктуру як таку, а безпосередньо на енергетичний фундамент держави, оскільки відключення електрики паралізує роботу державних сервісів, логістики та комунікацій. Тому у воєнний час кібернетичні операції стають складником стратегічного тиску.

Упродовж 2022–2025 рр. українські державні портали та системи електронного уряду (включно з порталами для подання заяв і доступу до соціальних послуг) неодноразово зазнавали DDoS-атак, сканування вразливостей. Навіть тимчасове блокування роботи таких сервісів створює труднощі для громадян, які залежать від електронного документообігу, реєстрацій чи отримання довідок. Це особливо критично у воєнний час, коли доступ до офлайн-держслужб обмежений і електронні сервіси стають основним каналом взаємодії громадян з державою.

У 2023–2025 рр. Європейське агентство з кібербезпеки ENISA фіксувало зростання складних атак на урядові системи ЄС, зокрема кампейни з компрометації облікових даних держслужбовців, DDoS-атаки на міністерські портали та спроби втрутитися у виборчі й адміністративні електронні сервіси (EU consistently targeted by diverse yet convergent threat groups, 2025).

Такі напади зазвичай координуються через широку мережу ботнетів та приховані троянські програми, що дають можливість тривалий час залишатися непоміченими. Ці атаки демонструють, що сучасні кіберагресори намагаються зламувати окремі сервіси й послабити державну спроможність реагувати на політичні та соціальні виклики, провокуючи недовіру до цифрових платформ, що стає загрозою для стабільності суспільства.

Спеціально організовані кібератаки під час воєнних дій не бувають випадковими, а часто є складниками стратегічних операцій проти держав. Вони можуть паралізувати ключові державні сервіси (енергетику, держпослуги, інфраструктурні мережі), що порушує повсякденне життя громадян та ускладнює оборонні зусилля; спричинити тимчасову недоступність цифрових платформ, від яких залежить доступ до соціальних виплат, медичних довідок, реєстрів і документів; послабити довіру громадян до цифрових послуг. В умовах війни це загрожує технічними збоями, соціальною нестабільністю, панікою та збільшенням рівня ризику шахрайства. Тому в сучасних умовах кібербезпека стала невід'ємним складником національної безпеки та стратегічної стійкості у військовому й у цивільному аспекті.

Висновки. Цифрова трансформація державного управління підкреслює роль електронної ідентифікації та цифрової документації як фундаменту цифрового суспільства, забезпечуючи підтвердження особи, правомірність документообігу та довіру між громадянами, державою і бізнесом. Досвід ЄС демонструє, що ефективні системи залежать від цифрової інфраструктури, нормативно-правової гармонізації та цифрової грамотності населення, а приклад Естонії підтверджує потенціал eID для розвитку цифрової державності. В Україні платформа «Дія», BankID НБУ та кваліфіковані підписи формують довіру до цифрових сервісів і поступово інтегруються з європейськими стандартами, але зберігаються ризики:

ISSN 2617-796X (print)
ISSN 2618-0049 (online)

централізація реєстрів, можливість витоку даних, соціальний інжиніринг, залежність від IT-інфраструктури та вразливості програмного забезпечення, що особливо критично в умовах війни.

Цілком можливо, що упродовж наступних 3–5 років масштабне впровадження мобільних рішень eID та інтеграція з European Digital Identity Wallet підвищать цифрову доступність державних сервісів, а розвиток кіберзахисту та цифрової грамотності населення мінімізує ризики витоку даних і шахрайства. За умови гармонізації українських стандартів із європейськими та розвитку резервної інфраструктури понад 80 % громадян зможуть користуватися електронними державними сервісами до 2030 р., що сприятиме формуванню стабільної цифрової довіри.

Отже, подальший розвиток eID в Україні потребує одночасного посилення нормативного регулювання, кіберзахисту, резервування IT-інфраструктури та інтеграції з європейськими стандартами, що забезпечить надійність цифрових сервісів і підвищить цифрову стійкість держави.

СПИСОК ПОСИЛАНЬ

Батке, Б., 2025. Як Естонія випередила всю Європу за рівнем цифровізації. *Deutsche Welle*, [online] 23 липня. Доступно: <https://www.dw.com/uk/ak-estonia-viperedila-vsu-evropu-zarivnem-cifrovizacii/a-73367362> [Дата звернення 01 березня 2026].

Верховна Рада України, 2022. *Про електронну ідентифікацію та електронні довірчі послуги*. Закон України, [online] 01 грудня, № 2801-IX. Доступно: <https://zakon.rada.gov.ua/laws/show/2155-19#Text> [Дата звернення 01 березня 2026].

Держава без черг і паперів: уже 23+ мільйони українців користуються Дією, 2025. *Дія*, [online] 8 жовтня. Доступно: <https://diia.gov.ua/news/derzhava-bez-cherh-i-paperiv-uzhe-23-miliony-ukraintsiv-korystuiutsia-diieiu?utm_source> [Дата звернення 01 березня 2026].

Жолобецький, С., 2026. Кількість електронних ідентифікацій у Системі BankID НБУ зросла на 25% до понад 109 млн шт. в 2025. *Українські Новини*, [online] 3 лютого. Доступно: <https://ukranews.com/ua/news/1132331-kilkist-elektronnyh-identyfikatsij-u-systemi-bankid-nbu-zrosla-na-25-do-109-4-mln-sht-v-2025> [Дата звернення 01 березня 2026].

Ковалів, М.В., Красницький, І.В., Пєтков, С.В., Єсімов, С.С., Корецька, В.В. та Явний, О.І., 2024. Правові засади електронної ідентифікації в Україні. *Міжнародний науковий журнал «Інтернаука». Серія: Юридичні науки*, [e-journal] 4 (74), с.21-26. https://doi.org/10.25313/2520-2308-2024-4-9696

Мирончук, Р., 2024. Унаслідок кібератаки витоку персональних даних із держреєстрів не підтверджено – Стефанішина. *Мінфін*, [online] 20 грудня. Доступно: <https://minfin.com.ua/ua/2024/12/20/141963921/> [Дата звернення 01 березня 2026].

Міністерство цифрової трансформації України, 2025. *Служба безпеки України та Офіс Генерального прокурора викрили учасників організованої злочинної групи, які незаконно отримували доступ до банківських акаунтів українців*. [online] 14 жовтня. Доступно: <https://thedigital.gov.ua/news/technologies/sluzba-bezpeky-ukrayiny-ta-ofis-heneralnoho-prokurora-vykryly-uchasnykiv-orhanizovanoyi-zlochynnoyi-hrupy-iaki-nezakonno-otrymuvaly-dostup-do-bankivskykh-akauntiv-ukrayintsiv> [Дата звернення 01 березня 2026].

Опанасенко, О., 2025. Кібератаки не було – масштабний збій онлайн-сервісів в Україні стався через аварію в дата-центрі. *Бабель*, [online] 26 квітня. Доступно: <https://babel.ua/news/117475-kiberataki-ne-bulo-masshtabniy-zbiy-onlayn-servisiv-v-ukrajini-stavsya-cherez-problemu-v-data-centri> [Дата звернення 01 березня 2026].
Прилуцький, С., 2024. Шахраї використали BankID, щоб увійти в «Дію»: українка поділилась своєю історією. *Апостроф*, [online] 17 грудня. Доступно: <https://apostrophe.ua/society/moshenniki-nauchilis-vzlamyivat-dyu-ukrainka-podelilas-svoey-istoriey.html?utm_source> [Дата звернення 01 березня 2026].
Худолій, Ю.С. та Дорош, В.В., 2025. Електронна ідентифікація та цифровий підпис як елементи захисту інформаційного середовища фінансових установ. В: *Економічна безпека: держава, регіон, підприємство.* Матеріали IX Міжнародної науково-практичної конференції, Полтава, Україна, 15 травня 2025 р. Полтава: Національний університет «Полтавська політехніка імені Юрія Кондратюка», с.172-176.
Arghire, I., 2026. European Commission Investigating Cyberattack. *SecurityWeek*, [online] February 9. Available at: <https://www.securityweek.com/european-commission-investigating-cyberattack/?utm_source> [Accessed 01 March 2026].
Birch, D., 2014. *Identity is the New Money*. London: London Publishing Partnership.
Castells, M., 2010. *The rise of the network society*. 2nd ed. Oxford: Blackwell Publishing.
Davies, E.J., 2025. Call for justice Ministry of Justice hit by brazen cyberattack as hackers steal 'significant amount' of personal dat. *The Scottish Sun*, [online] May 19. Available at: <https://www.thescottishsun.co.uk/news/14811241/ministry-cyber-attack-data> [Accessed 01 March 2026].
EU consistently targeted by diverse yet convergent threat groups, 2025. *European Union Agency for Cybersecurity*, [online] October 1. Available at: <https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups >[Accessed 01 March 2026].
Henley, J., Kassam, A. and Jones, S., 2025. Tens of millions across Spain and Portugal hit by huge power outage. *The Guardian*, [online] April 28. Available at: <https://www.theguardian.com/world/2025/apr/28/spain-portugal-power-outage> [Accessed 01 March 2026].
Pala, M., 2026. France reports data breach affecting 1.2 million bank accounts. *Anadolu Ajansı*, [online] February 18. Available at: <https://www.aa.com.tr/en/europe/france-reports-data-breach-affecting-12-million-bank-accounts/3834116> [Accessed 01 March 2026].
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014. *European Union*, [online] August 28. Available at: <https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng> [Accessed 01 March 2026].
70% of EU citizens used online public services in 2024, 2025. *Eurostat*, [online] February 26. Available at: <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250226-1?utm_source> [Accessed 01 March 2026].
Situation in cyberspace – October 2025, 2026. Republik of Estonia. *Information System Authority*, [online] February 03. Available at: <https://www.ria.ee/en/situation-cyberspace-october-2025> [Accessed 01 March 2026].
Vovk, M., Zaiats, O. and Yurkevych, Y., 2024. Legal regulation of electronic identification and electronic trust services in Ukraine: prospects for improvement and development under the conditions of harmonization with the law of the European Union. *Socio-Economic Relations in the Digital Society*, [e-journal] 1 (51), pp.117-126. https://doi.org/10.55643/ser.1.51.2024.558

ISSN 2617-796X (print)
ISSN 2618-0049 (online)

REFERENCES

Arghire, I., 2026. European Commission Investigating Cyberattack. *SecurityWeek*, [online] February 9. Available at: <https://www.securityweek.com/european-commission-investigating-cyberattack/?utm_source> [Accessed 01 March 2026].

Batke, B., 2025. Yak Estoniia vyperedyla vsiu Yevropu za rivnem tsyfrovizatsii [How Estonia has outpaced the rest of Europe in terms of digitalization]. *Deutsche Welle*, [online] July 23. Available at: <https://www.dw.com/uk/ak-estonia-viperedila-vsu-evropu-za-rivnem-cifrovizacii/a-73367362> [Accessed 01 March 2026].

Birch, D., 2014. *Identity is the New Money*. London: London Publishing Partnership.

Castells, M., 2010. *The rise of the network society*. 2nd ed. Oxford: Blackwell Publishing.

Davies, E.J., 2025. Call for justice Ministry of Justice hit by brazen cyberattack as hackers steal 'significant amount' of personal dat. *The Scottish Sun*, [online] May 19. Available at: <https://www.thescottishsun.co.uk/news/14811241/ministry-cyber-attack-data> [Accessed 01 March 2026].

Derzhava bez cherh i paperiv: uzhe 23+ miliony ukraintsiv korystuiutsia Diieiu [A State Without Queues and Papers: Already 23+ Million Ukrainians Use Diia], 2025. *Diia*, [online] October 8. Available at: <https://diia.gov.ua/news/derzhava-bez-cherh-i-paperiv-uzhe-23-miliony-ukraintsiv-korystuiutsia-diieiu?utm_source> [Accessed 01 March 2026].

EU consistently targeted by diverse yet convergent threat groups, 2025. *European Union Agency for Cybersecurity*, [online] October 1. Available at: <https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups>[Accessed 01 March 2026].

Henley, J., Kassam, A. and Jones, S., 2025. Tens of millions across Spain and Portugal hit by huge power outage. *The Guardian*, [online] April 28. Available at: <https://www.theguardian.com/world/2025/apr/28/spain-portugal-power-outage> [Accessed 01 March 2026].

Khudolii, Yu.S. and Dorosh, V.V., 2025. Elektronna identyfikatsiia ta tsyfrovyi pidpys yak elementy zakhystu informatsiinoho seredovyshcha finansovykh ustanov [Electronic identification and digital signature as elements of information environment protection of financial institutions]. In: *Ekonomichna bezpeka: derzhava, rehion, pidpryiemstvo* [Economic security: state, region, enterprise]. Proceedings of the IX International Scientific and Practical Conference, Poltava, Ukraine, May 15, 2025. Poltava: National University "Yuri Kondratyuk Poltava Polytechnic", pp.172-176.

Kovaliv, M.V., Krasnytskyi, I.V., Pietkov, S.V., Yesimov, S.S., Koretska, V.V. and Yavnyi, O.I., 2024. Pravovi zasady elektronnoi identyfikatsii v Ukraini [Legal basis of electronic identification in Ukraine]. International *Scientific Journal "Internauka". Series: "Juridical Sciences"*, [e-journal] 4 (74), pp.21-26. https://doi.org/10.25313/2520-2308-2024-4-9696

Ministry of Digital Transformation of Ukraine, 2025. *Sluzhba bezpeky Ukrainy ta Ofis Heneralnoho prokurora vykryly uchasnykiv orhanizovanoi zlochynnoi hrupy, yaki nezakonno otrymuvaly dostup do bankivskykh akauntiv ukraintsiv* [The Security Service of Ukraine and the Prosecutor General's Office have exposed members of an organized criminal group that illegally gained access to Ukrainians' bank accounts]. [online] October 14. Available at: <https://thedigital.gov.ua/news/technologies/sluzba-bezpeky-ukrayiny-ta-ofis-heneralnoho-prokurora-vykryly-uchasnykiv-orhanizovanoyi-zlochynnoyi-hrupy-iaki-nezakonno-otrymuvaly-dostup-do-bankivskykh-akauntiv-ukrayintsiv> [Accessed 01 March 2026].

Myronchuk, R., 2024. Unaslidok kiberataky vytoku personalnykh danykh iz derzhreiestriv ne pidtverdzheno – Stefanishyna [As a result of a cyberattack, personal data leakage from state

registers has not been confirmed – Stefanishyna]. *Minfin*, [online] December 20. Available at: <https://minfin.com.ua/ua/2024/12/20/141963921/> [Accessed 01 March 2026].
Opanasenko, O., 2025. Kiberataky ne bulo – masshtabnyi zbii onlain-servisiv v Ukraini stavsia cherez avariiu v data-tsentri [There was no cyberattack – a large-scale failure of online services in Ukraine occurred due to an accident in a data center]. *Babel*, [online] April 26. Available at: <https://babel.ua/news/117475-kiberataki-ne-bulo-masshtabniy-zbiy-onlayn-servisiv-v-ukrajini-stavsya-cherez-problemu-v-data-centri> [Accessed 01 March 2026].
Pala, M., 2026. France reports data breach affecting 1.2 million bank accounts. *Anadolu Ajansı*, [online] February 18. Available at: <https://www.aa.com.tr/en/europe/france-reports-data-breach-affecting-12-million-bank-accounts/3834116> [Accessed 01 March 2026].
Prylutskyi, S., 2024. Shakhrai vykorystaly BankID, shchob uviity v "Diiu": ukrainka podilylas svoieiu istoriieiu [Fraudsters used BankID to log in to "Diya": a Ukrainian woman shared her story]. *Apostrof*, [online] December 17. Available at: <https://apostrophe.ua/society/moshenniki-nauchilis-vzlamyivat-dyu-ukrainka-podelilas-svoey-istoriey.html?utm_source> [Accessed 01 March 2026].
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014. *European Union*, [online] August 28. Available at: <https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng> [Accessed 01 March 2026].
70% of EU citizens used online public services in 2024, 2025. *Eurostat*, [online] February 26. Available at: <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250226-1?utm_source> [Accessed 01 March 2026].
Situation in cyberspace – October 2025, 2026. Republik of Estonia. *Information System Authority*, [online] February 03. Available at: <https://www.ria.ee/en/situation-cyberspace-october-2025> [Accessed 01 March 2026].
Verkhovna Rada of Ukraine, 2022. *Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy* [On electronic identification and electronic trust service]. Law of Ukraine, [online] December 1, No. 2801-IX. Available at: <https://zakon.rada.gov.ua/laws/show/2155-19#Text> [Accessed 01 March 2026].
Vovk, M., Zaiats, O. and Yurkevych, Y., 2024. Legal regulation of electronic identification and electronic trust services in Ukraine: prospects for improvement and development under the conditions of harmonization with the law of the European Union. *Socio-Economic Relations in the Digital Society*, [e-journal] 1 (51), pp.117-126. https://doi.org/10.55643/ser.1.51.2024.558
Zholobetskyi, S., 2026. Kilkist elektronnykh identyfikatsii u Systemi BankID NBU zrosla na 25% do ponad 109 mln sht. v 2025 [The number of electronic identifications in the BankID System of the NBU increased by 25% to over 109 million in 2025]. *Ukrainski Novyny*, [online] February 3. Available at: <https://ukranews.com/ua/news/1132331-kilkist-elektronnyh-identyfikatsij-u-systemi-bankid-nbu-zrosla-na-25-do-109-4-mln-sht-v-2025> [Accessed 01 March 2026].

ISSN 2617-796X (print)
ISSN 2618-0049 (online)

UDK 002.1:004:303.094.4](477+4):004.056

Maryna Tsilyna,
PhD in Philological Sciences, Associate Professor,
Associate Professor at the Department
of Information Activities and Public Relations,
Kyiv National University of Culture and Arts,
Kyiv, Ukraine
e-mail: macilin@ukr.net
https://orcid.org/0000-0001-5339-5147

ELECTRONIC IDENTIFICATION AND DIGITAL DOCUMENTATION: EUROPEAN EXPERIENCE AND CYBERSECURITY CHALLENGES

The purpose of this research *is* to provide a comprehensive analysis of modern digitalisation processes in Ukrainian public administration, particularly in the fields of electronic identification and digital documentation, within the context of digital government development, the implementation of international eIDAS standards, and the integration of Ukrainian systems with European practices. This study aims to determine the role of electronic identification in ensuring accessibility to public services, promoting citizens' social mobility and fostering digital trust. Additionally, it assesses the main cybersecurity risks associated with the operation of digital government services and their impact on societal stability and security, as well as analyses prospects for the further integration of Ukrainian digital systems into the European and global digital space.

Research methodology. A combination of general scientific methods is applied: analytical method – to synthesise legal acts and academic sources on electronic identification and digital documentation; comparative method – to contrast Ukrainian and European experiences in implementing eID systems; systems approach – to study public sector digitalisation as a multidimensional process encompassing technological, legal, and social aspects; descriptive-review method – to record modern practices, incidents and research in electronic identification and digital government services; structural-functional analysis – to identify key tools, risks and cybersecurity challenges within the digital government ecosystem.

Scientific novelty. *The article provides a systematic review of modern practices in electronic identification and digit*al documentation in Ukraine in 2025, combining analysis of national strategies, legal frameworks, international eIDAS standards and European digital government practices. This approach allows the identification of key challenges, cybersecurity risks and prospects for integrating Ukrainian digital systems into the European and global digital space.

Conclusions*.* The digital transformation of public administration underscores the role of electronic identification (eID) and digital documentation as the foundation of a digital society, ensuring identity verification, legal validity of document flow and trust between citizens, the state, and businesses. European experience demonstrates that effective systems depend on digital infrastructure, legal harmonisation and digital literacy, while the Estonian example confirms the potential of eID for advancing digital statehood. In Ukraine, the "Diia" platform, NBU BankID and qualified electronic signatures are building trust in digital services and gradually integrating with European standards, although risks remain, including registry centralisation, potential data breaches, social engineering, dependence on IT infrastructure and software vulnerabilities, which are particularly critical in wartime conditions.

It is highly likely that over the next 3-5 years, large-scale deployment of mobile eID solutions and integration with the European Digital Identity Wallet will increase accessibility to public services, while the development of cybersecurity measures and digital literacy among the population will minimize data leakage and fraud risks. With the harmonisation of Ukrainian standards with European ones and the development of backup infrastructure, more than 80 % of citizens are expected to use electronic government services by 2030, fostering stable digital trust.

Therefore, further development of eID in Ukraine requires simultaneous strengthening of legal regulation, cybersecurity, IT infrastructure redundancy and alignment with the European standards in order to ensure the reliability of digital services and enhance the country's digital resilience.

Keywords*:* electronic identification; digital document;, BankID; cybersecurity; digital inequality; public services; digital sovereignty.

Надійшла 11.03.2026
Прийнята 06.04.2026
Стаття була вперше опублікована онлайн 29.05.2026

ISSN 2617-796X (print)
ISSN 2618-0049 (online)