УДК 004.056:342.9

Т.А. Присяжнюк

ЦИФРОВА ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Вінницький національний технічний університет

Анотація

У роботі досліджено роль цифрової ідентифікації як одного з ключових інструментів забезпечення інформаційної безпеки держави в умовах глобальної діджиталізації. Проаналізовано ефективність сучасних механізмів верифікації користувачів, зокрема застосунку Дія, кваліфікованого електронного підпису (КЕП), багатофакторної автентифікації та технології Mobile ID. Також обґрунтовано перехід від традиційних моделей захисту до концепції «нульової довіри» (Zero Trust), що базується на безперервному моніторингу та багаторівневій перевірці автентичності кожної дії в інформаційному просторі. Доведено, що інтеграція біометричних методів захисту та апаратних носіїв ключа створює надійний бар'єр проти кіберзагроз та несанкціонованого доступу до персональних даних громадян.

Ключові слова: цифрова ідентифікація, інформаційна безпека держави, застосунок Дія, електронний підпис, Mobile ID, багатофакторна автентифікація, Zero Trust.

Abstract:

The paper examines the role of digital identification as one of the key instruments for ensuring the information security of the state in the context of global digitalization. The effectiveness of modern user verification mechanisms has been analyzed, including the Diia application, qualified electronic signatures (QES), multi-factor authentication, and Mobile ID technology.The transition from traditional protection models to the Zero Trust concept has also been substantiated. This concept is based on continuous monitoring and multi-level authentication of every action within the information space.It has been demonstrated that the integration of biometric protection methods and hardware key storage devices creates a reliable barrier against cyber threats and unauthorized access to citizens' personal data.

Key words: digital identification, state information security, the Diia application, electronic signature, Mobile ID, multi-factor authentication, Zero Trust.

Вступ

У сучасну епоху глобальної цифровізації питання ідентифікації користувачів у кіберпросторі виходить далеко за межі технічного сервісу, стаючи стратегічним елементом інформаційної безпеки держави. Трансформація державних послуг у цифровий формат та переведення критично важливих реєстрів в онлайн-площину вимагають створення надійної системи верифікації особи, яка здатна протидіяти сучасним кіберзагрозам, маніпуляціям даними та несанкціонованому доступу. Ефективна цифрова ідентифікація є фундаментом довіри між громадянином і державою. Вона дозволяє не лише забезпечити безперервність надання адміністративних послуг, а й гарантувати цілісність національних інформаційних ресурсів. У контексті посилення гібридних загроз, розробка та впровадження стандартизованих протоколів перевірки автентичності користувачів стає запобіжником від кібертероризму та інструментом захисту цифрового суверенітету країни.

Результати дослідження

Сьогодні безпека держави – це не лише охорона кордонів, а й те, наскільки надійно ми захищені в інтернеті. Проведений аналіз показує, що без цифрової довіри та чіткої перевірки того, хто саме заходить у систему, державні сервіси просто не зможуть безпечно працювати. Оскільки хакери постійно шукають нові слабкі місця, держава має послідовно вдосконалювати способи розпізнавання користувачів. Сьогодні Україна формує комплексну систему цифрового захисту, використовуючи

відразу кілька сучасних інструментів, які суттєво ускладнюють несанкціоноване втручання в державні процеси та підвищують інформаційну стійкість суспільства. Основним інструментом юридичної верифікації став електронний підпис[1]. Він дозволяє не просто ідентифікувати особу, а й накласти цифровий «відбиток» на документ, будь-які зміни до якого можна виявити. Згідно з нормами Закону України «Про електронні довірчі послуги»[2], кваліфікований електронний підпис має таку ж юридичну силу, як і власноручний, що робить державний документообіг захищеним від підробок. Важливим кроком став розвиток застосунку Дія, який перетворив смартфон на повноцінний цифровий паспорт. Як зазначено на Офіційному порталі Дія, ключова особливість застосунку полягає в тому, що він не накопичує дані на серверах, а лише створює безпечний «канал» для їх відображення з державних реєстрів у момент запиту. Це значно знижує ризик масового витоку інформації при кібератаках.

Ще одним критичним елементом захисту є багатофакторна автентифікація (MFA)[3]. Цей метод передбачає, що для доступу до даних мало знати пароль – потрібно підтвердити особу ще одним способом, наприклад, через біометрію обличчя (FaceID) або спеціальний код у смартфоні. За даними Держспецзв'язку, використання кількох рівнів захисту дозволяє суттєво знизити кількість успішних спроб несанкціонованого доступу, оскільки зловмисникам майже неможливо одночасно вкрасти і пароль, і фізичний доступ до пристрою чи біометричних даних власника.

Паралельно з цим технологія Mobile ID[4] забезпечує найвищий рівень апаратної безпеки, оскільки особистий ключ користувача зберігається на спеціальній захищеній SIM-карті. Це робить Інтегровану систему електронної ідентифікації стійкою навіть до складних технічних маніпуляцій, оскільки ключ значно важче скопіювати чи віддалено викрасти без фізичного володіння карткою.

Поряд із суттєвими перевагами, сучасні системи ідентифікації мають і певні недоліки, які обмежують їхню ефективність. Зокрема, критичною є залежність від стабільного енергопостачання та доступу до мережі інтернет, що в умовах надзвичайних ситуацій може заблокувати доступ громадянина до державних сервісів. Також значним викликом залишається вразливість до методів соціальної інженерії, коли зловмисники маніпулюють довірою користувачів для отримання доступу до їхніх пристроїв. Окрім того, централізована архітектура державних баз даних створює потенційну загрозу «єдиної точки відмови», що вимагає постійного вдосконалення протоколів синхронізації та захисту вузлів передачі інформації.

Аналіз зазначених технологій дозволяє обґрунтувати перехід до моделі адаптивного «безшовного» захисту, у межах якої ідентифікація перестає бути одноразовою процедурою входу та перетворюється на безперервний процес контролю безпеки відповідно до підходу CARTA[5]. У такій парадигмі Дія.Підпис та Mobile ID доцільно розглядати як компоненти єдиної екосистеми, що забезпечує перевірку дій користувача в режимі реального часу згідно з принципами архітектури нульової довіри (Zero Trust Architecture). Перевага такої моделі полягає у відмові від використання лише статичних паролів на користь динамічної перевірки кожного запиту до державних інформаційних ресурсів. Технічна реалізація цього підходу базується на поєднанні інфраструктури відкритих ключів (PKI) з апаратними засобами захисту, зокрема Secure Enclave у смартфонах або захищеними SIM-картами. Це суттєво ускладнює несанкціонований доступ до приватних ключів користувача. Додатково може застосовуватися перевірка «живої» присутності (Liveness Check) за допомогою біометричних сенсорів, що знижує ризик використання викрадених облікових даних. Паралельно може використовуватися контекстуальна автентифікація, яка аналізує параметри пристрою, геолокацію та поведінкові особливості користувача для виявлення підозрілої активності.

Підсумовуючи, слід зазначити, що сучасна цифрова ідентифікація трансформувалася з простої процедури авторизації у складну багаторівневу систему та стала важливим елементом національної кібербезпеки та захисту цифрового суверенітету держави.

Висновки

В умовах глобальних цифрових трансформацій надійна ідентифікація користувачів перетворилася з допоміжного сервісу на фундаментальну складову інформаційної безпеки держави. Розвиток національної системи верифікації, що базується на поєднанні електронних підписів, мобільних технологій та багаторівневих методів перевірки, дозволив сформувати якісно нове захищене середовище для взаємодії громадян, бізнесу та владних інституцій. Ключовим результатом еволюції цих систем є перехід до сучасних моделей безпеки, де довіра до користувача не є статичною, а підтверджується динамічно на кожному етапі роботи з інформацією. Використання біометричних

даних та апаратних засобів захисту дозволяє ефективно протидіяти актуальним кіберзагрозам, забезпечуючи цілісність державних реєстрів і конфіденційність персональних даних навіть в умовах підвищеного ризику.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке електронний підпис та як він виглядає. Business Innovation Technology. [Електронний ресурс] URL: https://bit-ua.com/blog/shcho-take-elektronnyi-pidpys-ta-iak-vin-vyhliadaie(дата звернення: 22.04.2026).
2. Про електронну ідентифікацію та електронні довірчі послуги. Офіційний вебпортал парламенту України. [Електронний ресурс] URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 22.04.2026).
3. Що таке багатофакторна автентифікація (MFA)? - PROTECTIMUS. PROTECTIMUS. [Електронний ресурс] URL: https://www.protec timus.com/uk/what-is-multi-factor-authentication-mfa/ (дата звернення: 22.04.2026).
4. AVEST Mobile ID. Авест Україна. [Електронний ресурс] URL: https://www.avest.com.ua/avest-mobile-id-czyfrove-posvidchennya-osoby-shho-diye-na-bazi-mobilnogo-telefonu-i-zavzhdy-nayavne-u-vas-pry-sobi/(дата звернення: 22.04.2026).
5. Структура CARTA. Gartner. [Електронний ресурс] URL: https://safe.security/resources/insights/gartners-carta-frame work/ (дата звернення: 22.04.2026).

Присяжнюк Тетяна Анатоліївна – студентка факультету менеджменту та інформаційної безпеки, Вінницький національний університет, м. Вінниця, електронна пошта: pristaniya25@gmail.com

Науковий керівник: ***Грицак Анатолій Васильович*** – кандидат технічних наук з IT та кібербезпеки, Вінницький національний технічний університет, м. Вінниця, електронна пошта: grytsak.a.v@gmail.com

Prysiazhniuk Tetiana A. – Department of Information Systems Management and Security, Vinnytsia National Technical University, Vinnytsia, e-mail : pristaniya25@gmail.com

Supervisor: ***Hrytsak Anatoliy V.*** – candidate of Technical Sciences in IT and Cybersecurity, Vinnytsia National Technical University, Vinnytsia, e-mail : grytsak.a.v@gmail.com