

ЄВРОПЕЙСЬКИЙ ДОСВІД ЦИФРОВІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

EUROPEAN EXPERIENCE OF DIGITALISATION OF PUBLIC ADMINISTRATION IN THE NATIONAL SECURITY SYSTEM

Стаття присвячена дослідженню європейського досвіду цифровізації державного управління та її ролі у зміцненні національної безпеки. У ній висвітлюється інтеграція передових технологій, таких як штучний інтелект, блокчейн та платформи безпечного обміну даними, які значно підвищують стійкість та адаптивність систем державного управління. Актуальність цього дослідження зумовлена аналізом того, як цифрова трансформація підвищує адміністративну ефективність, забезпечує безпеку даних та сприяє зміцненню спроможності урядів протидіяти складним загрозам безпеці у взаємопов'язаному глобалізованому світі. Проаналізовано конкретні національні стратегії провідних європейських країн, таких як Естонія, Нідерланди, Німеччина та Франція, які впровадили інноваційні підходи до цифровізації в державному управлінні. Естонська платформа X-Road продемонструвала успіх у безпечному обміні даними та інтероперабельності, забезпечивши надійну основу для прийняття рішень у режимі реального часу. Реалізація принципу «єдиного вікна» в Нідерландах значно зменшила адміністративний тягар і зміцнила довіру до урядових процесів. Німеччина визначила кібербезпеку пріоритетом своєї національної стратегії, зосередившись на захисті критично важливої інфраструктури шляхом проактивного виявлення загроз і співпраці з приватним і академічним секторами. З'ясовано основні виклики, пов'язані з цифровізацією державного управління, включаючи технічні та інфраструктурні бар'єри, проблеми конфіденційності даних, питання транскордонної інтероперабельності та опір зміні у державних установах. Застарілі системи, несумісні з сучасними технологіями, та відсутність єдиних технічних стандартів перешкоджають створенню ефективних та інтегрованих систем. Правила захисту даних, такі як GDPR, мають важливе значення, але вимагають від урядів балансу між використанням даних для надання державних послуг і забезпеченням конфіденційності. Аргументовано перспективи подальших досліджень, які включають вивчення новітніх технологій, таких як квантові обчислення та машинне навчання, для цілей національної безпеки. Порівняльний аналіз цифрових стратегій в регіонах за межами Європи може запропонувати цінне розуміння глобальних тенденцій і інноваційних підходів. Було зроблено висновок, що діджиталізація, попри певні виклики, пропонує трансформаційний потенціал для зміцнення національної безпеки та підвищення ефективності управління. Вирішення цих проблем вимагає цілісного підходу, що поєднує технологічні, регуляторні та культурні виміри, забезпечуючи стійку та інклюзивну цифрову трансформацію в державному секторі.

Ключові слова: цифровізація, державне управління, цифровізація публічного управління, забезпечення цифровізації публічного управління, національна безпека, кібербезпека, інтероперабельність, штучний інтелект, блокчейн, захист даних, принцип

One-Only Principle, електронне урядування, транскордонне співробітництво, критична інфраструктура, цифрова трансформація, інформаційна безпека.

The article is devoted to the study of the European experience of digitalisation of public administration and its role in strengthening national security. It highlights the integration of advanced technologies, such as artificial intelligence, blockchain and secure data exchange platforms, which significantly increase the resilience and adaptability of public administration systems. The relevance of this study stems from the analysis of how digital transformation increases administrative efficiency, ensures data security, and contributes to strengthening the capacity of governments to counter complex security threats in an interconnected world. The article analyses specific national strategies of leading European countries, such as Estonia, the Netherlands, Germany and France, which have implemented innovative approaches to digitalisation in public administration. The Estonian X-Road platform has demonstrated success in secure data exchange and interoperability, providing a reliable basis for real-time decision-making. The implementation of the single window principle in the Netherlands has significantly reduced administrative burdens and strengthened trust in government processes. Germany has made cybersecurity a priority in its national strategy, focusing on protecting critical infrastructure through proactive threat detection and cooperation with the private and academic sectors. The main challenges associated with the digitalisation of public administration are identified, including technical and infrastructural barriers, data privacy concerns, cross-border interoperability issues, and resistance to change within government institutions. Outdated systems that are incompatible with modern technology and the lack of common technical standards hinder the creation of efficient and integrated systems. Data protection regulations, such as the GDPR, are important, but require governments to strike a balance between using data to provide public services and ensuring privacy. Prospects for further research, including the study of emerging technologies such as quantum computing and machine learning for national security purposes, are argued. A comparative analysis of digital strategies in regions outside Europe can offer valuable insights into global trends and innovative approaches. It was concluded that digitalisation, despite certain challenges, offers transformational potential for strengthening national security and improving governance. Addressing these challenges requires a holistic approach that combines technological, regulatory and cultural dimensions, ensuring sustainable and inclusive digital transformation in the public sector.

Key words: digitalisation, public administration, digitalization of the public administration, ensuring the digitization of public administration, national security, cybersecurity, interoperability, artificial intelligence, blockchain, data protection, One-Only Principle, e-government, cross-border cooperation, critical infrastructure, digital transformation, information security.

УДК 351:35.072
DOI <https://doi.org/10.32782/pma2663-5240-2025.45.28>

Яровой Т.С.

д. наук з держ. упр., доцент,
завідувач кафедри національної
безпеки, менеджменту та публічного
адміністрування
Чернігівський інститут Інформації,
бізнесу і права
Закладу вищої освіти «Міжнародний
Науково-технічний університет
імені академіка Юрія Бугая»

Обґрунтування актуальності теми дослідження. Цифровізація державного управління стала одним із найважливіших компонентів зміцнення систем національної безпеки, особливо – в контексті зростаючої складності глобальних загроз, таких як кібератаки, дезінформаційні кампанії та геополітична напруженість. Європейський Союз та його країни-члени продемонстрували значний прогрес у впровадженні передових цифрових технологій у державне управління, підвищуючи тим самим ефективність, прозорість та безпеку. Зазначене обумовлює актуальність вивчення точок перетину цифрових технологій та управління у галузі забезпеченні безпеки та стабільності держав.

Європейський досвід слугує орієнтиром для інших регіонів, передовсім, завдяки своїм комплексним стратегіям, таким як реалізація Європейського цифрового порядку денного, принципу «єдиного вікна» та надійної системи кібербезпеки. Завдяки таким ініціативам не лише спрощуються адміністративні процеси, але й зменшуються ризики, пов'язані з витоком даних та кіберзлочинністю, які стають все більш поширеними в цифрову епоху. Розуміння успіхів та викликів, з якими стикаються європейські країни, дає цінну інформацію для розробки ефективних моделей цифрового державного управління у всьому світі.

Крім того, досліджувана тема відповідає сучасним тенденціям у державному управлінні, де цифрова трансформація вже не є не обов'язковою, а стає реально необхідною для вирішення сучасних викликів безпеці.

Аналіз останніх досліджень і публікацій.

Огляд наявних досліджень, свідчить про значну увагу науковців до теми цифровізації державного управління в контексті зміцнення національної безпеки. Основна увага вчених присвячена впровадженню інтероперабельних систем, забезпеченню кібербезпеки та адаптації передових технологій, таких як блокчейн і штучний інтелект (Войціховський А., Гнатюк С., Грицишин В., Васильєва Н. В., Mamrot S., Ryszczak K., Бойко В. О., Семченко-Ковальчук О. Б., Костенюк Н., Макарова І., Пігарєв Ю., Сметаніна Л.). Періодично в центрі уваги науковців перебувають рішення країн ЄС, зокрема Естонії та Нідерландів, а також виклики, серед яких технічні бар'єри, конфіденційність даних та інституційний опір змінам.

Мета дослідження – здійснити аналіз європейського досвіду цифровізації державного управління та її ролі у зміцненні національної безпеки.

Основний зміст дослідження. Європейський Союз впроваджує комплексні стра-

тегії, спрямовані на просування цифровізації в державному управлінні, що має значний вплив на національну безпеку. Дані стратегії покликані сприяти інноваціям, підвищенню операційної ефективності та посиленню здатності урядів реагувати на нові загрози у взаємопов'язаному глобальному ландшафті. Цифрова стратегія ЄС, як наріжний камінь політики, зосереджена на створенні сталого і стійкого цифрового середовища, яке підтримує економічне зростання, соціальну згуртованість і безпеку [1]. Надаючи пріоритет цифровому суверенітету, стратегія гарантує, що держави-члени мають необхідну технологічну автономію для захисту критично важливої інфраструктури та захисту державних послуг від зовнішніх і внутрішніх загроз.

Ключовим аспектом підходу ЄС є акцент на структурах інтероперабельності, зокрема на Європейській структурі інтероперабельності EIF, яка слугує керівною структурою для узгодження адміністративних процесів і систем у державах-членах. EIF сприяє безперешкодному обміну даними між національними установами та установами на рівні ЄС, забезпечуючи швидке і скоординоване реагування на потенційні загрози безпеці [2]. Його багаторівнева структура, що охоплює правову, організаційну, семантичну і технічну інтероперабельність, забезпечує стандартизацію цифрових рішень, залишаючись при цьому адаптованою до унікальних вимог окремих країн. Інтероперабельна екосистема зменшує надмірність, підвищує прозорість і посилює здатність органів державного управління виявляти і пом'якшувати кіберзагрози, які можуть поставити під загрозу національну безпеку.

Європейський цифровий порядок денний, ще одна важлива ініціатива, зробила значний внесок у зміцнення національної безпеки шляхом інтеграції цифрових технологій у державне управління. Порядок денний наголошує на розвитку безпечних каналів зв'язку, модернізації державних послуг та впровадженні передових технологій, таких як штучний інтелект і блокчейн. Сприяючи цифровій інклюзії та забезпечуючи доступ до високоякісного інтернет-зв'язку, порядок денний підвищує стійкість як державних установ, так і суспільства в цілому до кібератак та інших вразливостей у сфері безпеки.

Реалізація цих стратегій проявляється у впровадженні безпечних транскордонних електронних послуг, які покладаються на передові методи автентифікації та стандарти шифрування для захисту конфіденційних даних. Такі країни, як Естонія, продемонстрували ефективність цих заходів за допомо-

гою надійних платформ цифрового врядування, які уможливають обмін інформацією в режимі реального часу та спільне прийняття рішень [3]. Аналогічним чином, ініціативи з підвищення цифрової грамотності та обізнаності з питань кібербезпеки серед державних службовців та громадян ще більше підкреслюють відданість ЄС створенню безпечного цифрового середовища.

Естонія виділяється як одна з перших країн в інфраструктурі електронного уряду, демонструючи неабиякий успіх в інтеграції цифрових рішень в державне управління для посилення національної безпеки та ефективності управління. Центральне місце в цифровій екосистемі Естонії займає платформа X-Road – захищений рівень обміну даними, який забезпечує безперешкодний і зашифрований зв'язок між різними державними установами та суб'єктами приватного сектору [4]. Інноваційна платформа не лише забезпечує сумісність між системами, але й надає стійку основу, здатну протистояти кіберзагрозам, таким чином захищаючи конфіденційну інформацію та підвищуючи операційну надійність.

Інфраструктура X-Road дозволяє децентралізовано зберігати дані та обмінюватися ними, гарантуючи, що інформація не буде сконцентрована в одному сховищі, тим самим зменшуючи ризики витоку даних або збоїв у роботі системи. Урядові установи використовують цю платформу для доступу та обміну даними в режимі реального часу, що дозволяє координувати процеси прийняття рішень під час критичних ситуацій, таких як національні надзвичайні ситуації або кіберінциденти. Прозорість і відстежуваність, закладені в системі, ще більше підвищують довіру громадськості до діяльності уряду, оскільки громадяни можуть контролювати, хто і з якою метою отримує доступ до їхніх персональних даних.

Успіх Естонії в безпечному обміні даними підкреслюється її здатністю підтримувати безперебійне управління навіть в умовах зовнішніх загроз. Широке впровадження в країні цифрових ідентифікаторів і безпечних методів автентифікації дозволило ефективно надавати послуги з дотриманням суворих протоколів безпеки. Цифровий підхід поширюється на різні сектори, включаючи охорону здоров'я, освіту та оборону, гарантуючи, що життєво важливі послуги залишаються в робочому стані і захищені від зовнішніх збоїв.

Міжвідомча комунікація в Естонії значно виграє від інтероперабельності, яку забезпечує платформа X-Road, що дозволяє швидко реагувати на складні виклики безпеці. Чи

то координація зусиль з кіберзахисту, чи то сприяння транскордонному співробітництву з іншими європейськими країнами – ця інфраструктура є прикладом того, як технології можуть підвищити гнучкість і стійкість систем державного управління. Естонська модель електронного урядування слугує еталоном для демонстрації того, як стратегічна цифровізація може зміцнити національну безпеку, забезпечуючи при цьому ефективне надання державних послуг.

Нідерланди позиціонують себе як лідера в цифровому державному управлінні завдяки успішному впровадженню Принципу одного разу надання даних Once-Only Principle, OOP – ключової ініціативи, спрямованої на зменшення адміністративного тягаря та підвищення безпеки даних. Гарантуючи, що громадяни та бізнес надають інформацію державним органам лише один раз, цей принцип усуває надлишковий збір даних, мінімізує неефективність та значно зменшує ризики, пов'язані з дублюванням даних [5]. Надійна цифрова інфраструктура, що підтримує OOP, дозволяє безперешкодно обмінюватися даними між державними установами, зберігаючи при цьому високі стандарти безпеки та конфіденційності.

Даний принцип ґрунтується на інтероперабельних системах, які дозволяють уповноваженим органам отримувати доступ до існуючих даних без необхідності повторного введення даних користувачами, тим самим впорядковуючи адміністративні процеси та сприяючи зміцненню довіри між громадянами та державою. Правові та технічні рамки, що лежать в основі ПВУ в Нідерландах, надають пріоритет безпечному обміну даними та дотриманню суворих законів про конфіденційність, забезпечуючи відповідність національним нормам та нормам Європейського Союзу [6]. Ініціатива призвела до помітного зниження бюрократичної неефективності, економії витрат на державне управління та посилення безпеки за рахунок мінімізації надмірності зберігання даних, якою можуть скористатися зловмисники.

Німеччина схильна інтегрувати кібербезпеку, як фундаментальний аспект своєї стратегії цифровізації, визнаючи критичну важливість захисту національної інфраструктури у все більш взаємопов'язаному світі. Зусилля були зосереджені на захисті критично важливих секторів, включаючи енергетику, охорону здоров'я і транспорт, від складних кіберзагроз. Впровадження надійної системи кібербезпеки та використання найсучасніших технологій підкреслює відданість Німеччини справі захисту своєї цифрової інфраструктури.

Стратегія цифровізації країни включає такі ініціативи, як Національна стратегія кібербезпеки, яка наголошує на проактивному виявленні загроз, безпечній обробці даних та співпраці між державним і приватним секторами. Для забезпечення стійкості критично важливої інфраструктури були розроблені вдосконалені системи моніторингу та протоколи реагування на інциденти. Завдяки цим заходам вирішуються не лише нагальні проблеми безпеки, але й закладається фундамент для довгострокової цифрової стійкості, що дозволяє Німеччині ефективно реагувати на нові кіберзагрози, що еволюціонують.

Зосередженість Німеччини на кібербезпеці доповнюється інвестиціями в дослідження та інновації, спрямовані на розробку нових технологій для посилення цифрової безпеки. Співпраця між державними установами, науковими колами та приватним сектором призвела до розробки рішень, спрямованих на передбачення та пом'якшення ризиків, що виникають [7]. Дані зусилля підкреслюють важливість багатогранного підходу, який поєднує технічні гарантії, правові рамки та міжсекторальну співпрацю для забезпечення цілісності національної інфраструктури.

Франція впроваджує цифрову трансформацію в державному управлінні, інтегруючи передові технології, такі як штучний інтелект і блокчейн, для покращення управління та зміцнення національної безпеки. Застосування ШІ дозволило державним установам аналізувати величезні обсяги даних з безпрецедентною швидкістю і точністю, підтримуючи більш обґрунтовані процеси прийняття рішень і підвищуючи ефективність операцій з безпеки. Предиктивна аналітика на основі ШІ все частіше використовується для виявлення потенційних загроз, оптимізації розподілу ресурсів і підвищення оперативності реагування сил безпеки.

Технологія блокчейн ще більше посилила цілісність і прозорість державного управління, забезпечивши захист записів від підробки та безпечні механізми транзакцій. У таких сферах, як системи голосування, верифікація особи та державні закупівлі, блокчейн гарантує, що конфіденційні дані залишаються в безпеці, одночасно підвищуючи довіру громадськості до урядових процесів [8]. Використовуючи ці технології, Франція продемонструвала свою здатність адаптуватися до викликів цифрової епохи, надаючи пріоритет національній безпеці.

Зусилля Франції у сфері цифровізації також поширюються на зміцнення міжнародного співробітництва у сфері кібербезпеки та управління даними. Завдяки активній участі в

ініціативах Європейського Союзу та глобальних партнерствах Франція зробила свій внесок у розробку спільних стандартів і протоколів, які посилюють колективну безпеку взаємопов'язаних націй. Підхід країни підкреслює трансформаційний потенціал цифрових технологій у побудові стійких, ефективних і безпечних систем державного управління, здатних протистояти сучасним викликам безпеки.

Цифровізація державного управління пов'язана з численними викликами, які необхідно вирішити, щоб забезпечити успішне впровадження та сталість ініціатив цифрової трансформації. Серед найбільш значних перешкод – технічні та інфраструктурні бар'єри, які часто виникають через застарілі системи, несумісні з сучасними технологіями. Відсутність єдиних технічних стандартів у державних установах ще більше ускладнює зусилля зі створення інтегрованих та ефективних цифрових систем [9]. Обмежений доступ до високошвидкісного інтернету та недостатні технологічні ресурси в сільській місцевості або районах з низьким рівнем обслуговування загострюють ці проблеми, перешкоджаючи справедливій цифровізації та створюючи нерівність у наданні послуг.

Питання конфіденційності та захисту даних є ще одним важливим викликом, особливо в контексті зростаючих кіберзагроз та підвищення обізнаності громадськості щодо зловживань з персональною інформацією. Уряди повинні враховувати складні правові та етичні міркування, щоб забезпечити дотримання суворих правил захисту даних, таких як Загальний регламент про захист даних GDPR в Європейському Союзі [10]. Баланс між використанням даних для покращення державних послуг і захистом приватного життя є делікатним, що вимагає надійних заходів безпеки і прозорих механізмів управління для зменшення ризиків і зміцнення довіри громадськості.

Проблеми транскордонної інтероперабельності ще більше ускладнюють цифровізацію державного управління, особливо в таких регіонах, як Європейський Союз, де безперешкодна співпраця між країнами-членами має важливе значення для вирішення спільних проблем. Різноманітність правових, технічних і семантичних стандартів у різних країнах створює значні перешкоди для ефективного обміну даними та спільного управління. Відсутність загальноприйнятих протоколів і фрагментарне впровадження цифрових технологій перешкоджають створенню цілісних та інтероперабельних систем, здатних підтримувати багатонаціональні ініціативи.

Опір змінам у державних установах є додатковим бар'єром на шляху цифрової трансформації. Інституційна інерція, зумовлена перевагою традиційних процесів і скептичним ставленням до нових технологій, може затримувати впровадження інноваційних рішень. Державні службовці можуть не мати необхідних цифрових навичок або сприймати технологічні зміни як загрозу своїй ролі, що призводить до небажання впроваджувати реформи.

Висновки та перспективи подальших досліджень. Цифровізація державного управління в контексті національної безпеки є трансформаційним процесом, який змінив спосіб функціонування урядів та реагування на сучасні виклики. Європейські країни продемонстрували різний ступінь успіху в реалізації цифрових стратегій, а такі ініціативи, як Європейський цифровий порядок денний, Принцип одноразового використання та рамки інтероперабельності, такі як Європейська рамка інтероперабельності, слугують орієнтирами для найкращих світових практик. Такі зусилля значно підвищили адміністративну ефективність, покращили безпеку даних і зміцнили спроможність протистояти комплексним загрозам безпеці.

Інтеграція передових технологій, таких як штучний інтелект, блокчейн і платформи безпечного обміну даними, ще більше посилила стійкість і гнучкість систем державного управління. Такі країни, як Естонія, Нідерланди, Німеччина та Франція, є прикладом того, як стратегічні інвестиції в цифрову інфраструктуру та інноваційні рішення можуть принести значні вигоди з точки зору національної безпеки та ефективності управління. Незважаючи на ці успіхи, такі виклики, як технічні та інфраструктурні бар'єри, занепокоєння щодо конфіденційності даних, проблеми транскордонної інтероперабельності та інституційний опір змінам, підкреслюють складність досягнення безперебійної цифровізації в різних адміністративних ландшафтах.

Перспективи подальших досліджень полягають у вивченні нових технологій та їхнього потенціалу для вирішення існуючих проблем і створення нових можливостей для державного управління. Майбутні дослідження можуть бути зосереджені на застосуванні квантових обчислень для захисту критичної інфраструктури, ролі машинного навчання в прогностичній аналітиці для національної безпеки, а також на етичних наслідках впровадження цих технологій в державному управлінні. Крім того, порівняльний аналіз стратегій цифровізації в неєвропейських регіонах може надати цінну інформацію про глобальні тенденції та інноваційні підходи.

Незважаючи на значний прогрес у цифровізації державного управління, необхідні подальші дослідження та інновації для вирішення поточних проблем і адаптації до динамічного ландшафту технологічного прогресу та загроз безпеці. Перспективний підхід, що поєднує технологічні, регуляторні та культурні аспекти, матиме вирішальне значення для формування майбутнього державного управління в цифрову епоху.

ЛІТЕРАТУРА:

1. Войціховський А. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права*. 2018. № 53. С. 26–37. URL: <https://www.academia.edu/39795468>
2. Гнатюк С. Європейський досвід нормативно-проектного забезпечення розвитку інформаційного суспільства. *Національний інститут стратегічних досліджень*. 2014. С. 76 URL: <https://niss.gov.ua/sites/default/files/2015-02/Gnatyuk-59546.pdf>
3. Грицишин В. Е-урядування Естонії: досвід для України. *Матеріали IV Міжнародної студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання»*. 2021. С. 219–220. URL: https://elartu.tntu.edu.ua/bitstream/lib/36103/2/MSNTK_2021_Hrytsyshyn_V-E_government_of_Estonia_219-220.pdf
4. Васильєва Н. В. Досвід Естонії у наданні електронних послуг населенню. *Державне управління: удосконалення та розвиток*. 2013. № 11. URL: <http://www.dy.nayka.com.ua/?op=1&z=650>.
5. Once-Only Principle: A System Breakthrough for the EU's Digital Single Market. *European Commission*. 2020. URL: https://commission.europa.eu/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-11-05_en.
6. Mamrot, S., Ryzyszczak, K. Implementation of the 'Once-Only' Principle in Europe – National Approach. In: Krimmer, R., Prentza, A., Mamrot, S. (eds) *The Once-Only Principle. Lecture Notes in Computer Science*, 2021, vol 12621. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-79851-2_2
7. В. О. Бойко. Державно-приватне партнерство у сфері кібербезпеки: кейс Німеччини. *Національний інститут стратегічних досліджень*. 2018. URL: <https://niss.gov.ua/sites/default/files/2018-01/Germany-7f497.pdf>
8. Семченко-Ковальчук, О. Б. Використання блокчейну в публічному управлінні: трансформація технологічних можливостей. *Economic Synergy*, 2023, (2), 62–73. URL: <https://doi.org/10.53920/ES-2023-2-5>
9. Костенюк Н., Макарова І., Пігарєв Ю., Сметаніна Л. Цифровізація публічного управління: вітчизняний досвід. *Теоретичні та прикладні питання державотворення*. 2021. № 26. С. 41–50 URL: <http://taais.oridu.odessa.ua/article/view/239001>
10. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). *Офіційний веб-сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text