УДК 351:35.072
DOI https://doi.org/10.32782/TNU-2663-6468/2025.1/29

Яровой Т.С.
Чернігівський інститут інформації, бізнесу і права
ЗВО «Міжнародний Науково-технічний університет імені академіка Юрія Бугая»

РЕТРОСПЕКТИВА ЦИФРОВІЗАЦІЇ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ КРІЗЬ ПРИЗМУ ПУБЛІЧНОГО УПРАВЛІННЯ

Стаття присвячена дослідженню історичної траєкторії цифровізації в системі національної безпеки з акцентом на її еволюцію крізь призму державного управління. Дослідження продемонструвало трансформаційну роль технологій у протидії новим загрозам безпеці та збереженні стратегічних переваг у динамічному, мінливому глобальному ландшафті. Простежуючи ключові етапи, такі як інтеграція комп'ютерів в оборонні системи, розробка механізмів командування і управління в режимі реального часу і прийняття передових заходів з кібербезпеки, в дослідженні розглядається, як цифрові інновації змінили систему управління та операційні рамки національної безпеки.Досліджено механізми, за допомогою яких державне управління інтегрувало цифрові інструменти для посилення національної безпеки, з акцентом на створенні агентств кібербезпеки, прогностичній аналітиці та штучному інтелекті. В аналізі розглянуто, як такі країни, як Естонія, США та Сінгапур, впровадили ефективні стратегії захисту критично важливої інфраструктури та налагодили міжсекторальну співпрацю. Висновки наголошують на важливості адаптивної політики, інноваційних технологій та скоординованих зусиль для зменшення ризиків, пов'язаних з кіберзагрозами, та забезпечення ефективного врядування. З'ясовано конкретні виклики та можливості, що виникають у зв'язку з цифровізацією систем національної безпеки. Дослідження виявило такі проблеми, як швидка еволюція кіберзагроз, етичні наслідки технологій спостереження і глобальний цифровий розрив, які вимагають цілеспрямованих політичних заходів і міжнародного співробітництва. Дослідження також розкрило потенціал нових технологій, включаючи блокчейн і квантові обчислення, для революційних змін у державному управлінні та національній безпеці. Порівняльний аналіз різних підходів до врядування ілюструє розмаїття рішень і кращих практик, які можуть бути адаптовані до різних геополітичних і соціально-економічних контекстів.Обґрунтовано необхідність подальших досліджень на перетині цифровізації та державного управління з акцентом на довгострокові наслідки технологічного прогресу для національної безпеки. Дослідження підкреслює потребу в інноваційних стратегіях управління, які збалансовують переваги цифровізації з ризиками кіберзалежності та вразливості даних.

Ключові слова: *цифровізація, національна безпека, державне управління, цифровізація публічного управління, забезпечення цифровізації публічного управління, кібербезпека, електронне урядування, кризовий менеджмент, інтеграція політики, моделі управління, нові технології, інформаційна війна, геополітичні загрози, цифрова трансформація, глобальні тенденції безпеки.*

Постановка проблеми. В епоху, коли цифрові технології глибоко інтегровані в усі аспекти управління та безпеки, роль державного управління у забезпеченні ефективного та безпечного впровадження цих технологій важко переоцінити. Цифровізація докорінно трансформувала механізми забезпечення національної безпеки, запровадивши передові інструменти для моніторингу, аналізу, прийняття рішень та реагування на загрози.Зростаюча витонченість кіберзагроз – від атак на критичну інфраструктуру до дезінформаційних кампаній – вимагає надійної та адаптивної системи державного управління для захисту національних інтересів. Це особливо важливо, оскільки уряди все більше покладаються на цифрові системи для управління чутливою інформацією, забезпечення безпеки кордонів і підтримки стійкості основних послуг. Ретроспективний аналіз цифровізації в системі національної безпеки дає цінну інформацію про еволюцію цих практик, висвітлюючи як успіхи, так і виклики, з якими стикаються держави у використанні технологій для зміцнення безпеки.Критична важливість цифрової стійкості в умовах геополітичної напруженості, економічної нестабільності та технологічних порушень, додатково обумовлює актуальність

дослідження. Крім того, воно має практичне значення для політиків, експертів з питань безпеки та державних службовців, дозволяючи їм розробляти обґрунтовані стратегії, які підвищують ефективність і дієвість систем національної безпеки в умовах цифрового ландшафту, що швидко розвивається.

Аналіз останніх досліджень і публікацій. Огляд досліджень і публікацій свідчить про значну увагу до питань цифровізації в національній безпеці та ролі державного управління у забезпеченні ефективного впровадження технологій. Дослідники акцентують на впливі цифрових інструментів на управління ризиками, адаптацію політик до викликів кібербезпеки та інтеграцію інноваційних підходів, таких як штучний інтелект і блокчейн, у стратегії безпеки (Ткач М., Ясенко С., Бойко Р., Дриньов Д., Мосов С. П., Сєлюков О. В., Бхарвадж А., Каушик К., Бігняк П. І., Михальчук В. М., Білко С., Мельниченко Г., Білоус С., Архипова Є. О.). Ряд науковців відзначають потребу у міжвідомчій співпраці та міжнародній інтеграції.

Постановка завдання. Мета дослідження – проаналізувати історичну складову цифровізації в системі національної безпеки через призму державного управління, зосередившись на її розвитку, сучасному застосуванні та майбутньому потенціалі.

Виклад основного матеріалу. Історичний розвиток цифровізації в системі національної безпеки – це трансформаційний шлях, який характеризується поступовою інтеграцією передових технологій для протидії новим загрозам і викликам. Цей шлях розпочався з упровадження комп'ютерів в оборонні системи в середині XX-го століття, що стало початковим етапом цифрової революції в операціях з забезпечення безпеки. Перші комп'ютери, такі як ENIAC в США, використовувались в основному для військових розрахунків і криптографічного аналізу, що заклало основу для використання обчислювальних потужностей в удосконаленні процесів прийняття рішень в рамках оборонних механізмів [1]. Використання цих систем революціонізувало військові стратегії, уможлививши швидшу обробку даних і підвищивши точність операцій.Під час холодної війни швидкий розвиток технологій ще більше прискорив діджиталізацію у сфері національної безпеки. Розвиток систем командування і управління, в тому числі напівавтоматичного наземного середовища SAGE в США, продемонстрував інтеграцію можливостей обробки даних в реальному часі з радіолокаційними системами для моніторингу і реагування на потенційні повітряні загрози. Період також став свідком розвитку супутникових технологій, які розширили можливості спостереження і розвідки, дозволивши країнам збирати важливу розвідувальну інформацію за межами своїх кордонів [2]. Дані інновації підкреслили зростаючу залежність від цифрових систем для збереження стратегічної переваги. Закінчення холодної війни ознаменувало поворотний момент у застосуванні цифрових технологій в національній безпеці, зумовлений появою Інтернету і зростанням важливості кібербезпеки. Інтернет, який спочатку розроблявся як військовий проект в рамках мережі Агентства передових дослідницьких проектів ARPANET [3], перетворився на глобальну комунікаційну інфраструктуру, змінивши динаміку обміну інформацією і ведення війни. Поява взаємопов'язаних мереж призвела до появи нових вразливостей, оскільки противники почали використовувати кіберпростір для ведення шпигунства, диверсій та інформаційної війни. Дана ситуація зумовило необхідність розробки надійних заходів кібербезпеки для захисту критично важливих об'єктів інфраструктури, конфіденційної інформації та національних інтересів.Однією з важливих віх цього періоду стало створення агентств і структур з кібербезпеки, таких як Комп'ютерна група реагування на надзвичайні ситуації CERT у 1988 році, яка була створена у відповідь на черв'як Морріса, один з перших великих кіберінцидентів. Подія висвітлила потенційні загрози, які несе в собі шкідливе програмне забезпечення, і підкреслила необхідність скоординованих зусиль для зменшення кіберризиків [4]. У наступні роки уряди країн світу почали інвестувати значні кошти в дослідження кібербезпеки та розробку передових механізмів захисту, включаючи брандмауери, системи виявлення вторгнень і технології шифрування.Історичний розвиток цифровізації в національній безпеці відображає безперервний процес адаптації та інновацій, зумовлений необхідністю протистояти новим загрозам і зберігати стратегічну перевагу. Від початкового використання примітивних комп'ютерів до комплексної інтеграції штучного інтелекту і систем кібербезпеки, цифровізація національної безпеки докорінно змінила спосіб, в який уряди вирішують проблеми в умовах глобального ландшафту, що швидко змінюється [5]. Прогрес підкреслює вирішальну роль технологічного прогресу в підвищенні ефективності і стійкості систем національної безпеки.Роль держав-

ного управління в адаптації моделей управління до цифрових досягнень має вирішальне значення у вирішенні зростаючих складнощів національної безпеки в епоху технологічних перетворень. Системи державного управління зазнали значної еволюції, щоб інтегрувати цифрові інструменти, забезпечуючи їхню відповідність вимогам сучасного врядування та імперативам безпеки. Такі адаптації відображають не лише мінливий характер загроз, але й можливості, які надає розвиток цифрових технологій, що докорінно змінили механізми, за допомогою яких уряди діють і захищають свої національні інтереси.Моделі управління в державному управлінні дедалі більше охоплюють цифровізацію, як центральний компонент стратегічного планування та оперативного виконання. Традиційні ієрархічні структури, що характеризуються жорсткими централізованими процесами прийняття рішень, поступово замінюються або доповнюються більш гнучкими та адаптивними моделями, які надають пріоритет гнучкості та оперативності. Завдяки таким змінам стало можливим впровадження цифрових платформ, які уможливлюють обмін даними в режимі реального часу, міжвідомчу співпрацю та прийняття рішень на основі фактичних даних, підвищуючи таким чином загальну ефективність та результативність врядування [6]. Впровадження платформ електронного урядування за підтримки інтегрованих інформаційних систем змінило спосіб управління ресурсами, координації дій і надання послуг державними адміністраціями, забезпечивши вищий рівень прозорості, підзвітності та стійкості перед обличчям нових викликів безпеці.Інтеграція політики виконує центральну роль у наданні державним адміністраторам можливості впроваджувати цифрові інструменти, що сприяють зміцненню національної безпеки. Уряди дедалі більше визнають необхідність включення цифровізації в основу своєї політики, що призводить до формулювання комплексних стратегій, які враховують як можливості, так і ризики, пов'язані з технологічним прогресом. Перед державними адміністраторами стоїть завдання розробляти та впроваджувати політику, яка не лише сприяє впровадженню цифрових технологій, але й забезпечує їхнє безпечне та етичне застосування [7]. Виконання цього дуального завдання вимагає глибокого розуміння взаємозв'язку між технологіями, управлінням і безпекою, а також здатності орієнтуватися в складних регуляторних ландшафтах і сприяти співпраці між різними зацікавленими сторонами. Впровадження цифрових інструментів в урядування також вимагає створення спеціалізованих інституцій та нормативно-правової бази, які підтримують їх впровадження та нагляд за ними. Створення агентств з кібербезпеки, цифрових робочих груп та органів захисту даних підкреслює важливу роль державного управління в управлінні ризиками, пов'язаними з цифровізацією. Вони відповідають за розробку стандартів, проведення оцінки ризиків і координацію національних заходів реагування на кіберзагрози, забезпечуючи тим самим безпеку і цілісність критично важливих інформаційних інфраструктур. Державні адміністратори відіграють важливу роль у зміцненні міжнародної співпраці з питань кібербезпеки, беручи участь у таких ініціативах, як Будапештська конвенція про кіберзлочинність та багатосторонні рамки в рамках таких організацій, як ООН і НАТО, спрямовані на посилення глобальної кіберстійкості.Цифрові досягнення також трансформували роль державних адміністраторів у забезпеченні національних інтересів завдяки впровадженню предиктивної аналітики та штучного інтелекту, які дають змогу урядам передбачати та пом'якшувати потенційні загрози. Інтеграція цих технологій у процеси державного управління сприяла розробці систем раннього попередження, які використовують величезні обсяги даних для виявлення нових ризиків та проактивного втручання . Від державних службовців дедалі частіше вимагають розвивати компетенції в управлінні такими технологіями, забезпечуючи їх ефективне застосування, враховуючи при цьому проблеми, пов'язані з конфіденційністю, етичними міркуваннями та довірою громадськості. Впровадження цифрових інструментів також призвело до значного прогресу у сфері управління кризовими ситуаціями, де державне управління відіграє життєво важливу роль у координації реагування на надзвичайні ситуації та забезпеченні безперервності надання основних послуг. Цифрові платформи та геопросторові технології розширили можливості урядів щодо моніторингу, прогнозування та своєчасного й ефективного реагування на стихійні лиха, пандемії та інші кризові ситуації [8]. Інтеграція цих інструментів у державне управління не лише покращила обізнаність про ситуацію, але й уможливила більш ефективну комунікацію з громадськістю, сприяючи тим самим підвищенню стійкості та соціальної згуртованості.Завдяки адаптації моделей управління та інтеграції цифрових інструментів державне управління продемонструвало свою здатність розвиватися у відповідь на вимоги світу, який стає

все більш взаємопов'язаним і технологічно розвиненим. Використовуючи потенціал цифрових досягнень, державні адміністратори відіграють вирішальну роль у зміцненні національної безпеки, стимулюванні інновацій та забезпеченні сталого розвитку систем управління, здатних відповідати на виклики XXI століття. Трансформація, що триває, підкреслює важливість державного управління як динамічного та важливого компонента сучасного державотворення. Вивчення реальних кейсів демонструє, як країни використовують цифрові досягнення для зміцнення національної безпеки за допомогою інноваційних систем державного управління. Кожен кейс підкреслює важливість стратегічного планування, технологічної інтеграції та проактивного врядування у вирішенні багатогранних викликів, пов'язаних з цифровими загрозами, одночасно використовуючи можливості, які пропонує технологічний прогрес.Естонська Республіка часто наводиться як провідний приклад успішного цифрового врядування, особливо в контексті національної безпеки та стійкості до кіберзагроз. Після серії руйнівних кібератак у 2007 році, спрямованих на урядові веб-сайти, фінансові установи та основні послуги, Естонія провела комплексну модернізацію своєї інфраструктури цифрової безпеки. Ці зусилля призвели до створення екосистеми електронного урядування, яка базується на захищеній системі цифрової ідентифікації, технології блокчейн для забезпечення цілісності даних і децентралізованих центрах обробки даних для запобігання перебоїв у наданні послуг під час потенційних атак [9]. Впровадження системи X-Road дозволяє безперешкодно та безпечно обмінюватися даними між державними та приватними організаціями, забезпечуючи безперервність надання критично важливих послуг навіть під час надзвичайних ситуацій. Крім того, Естонія інституціоналізувала свої зусилля з кібербезпеки, створивши Естонське управління інформаційних систем RIA і Центр передового досвіду НАТО з питань спільного кіберзахисту, зміцнивши свою позицію світового лідера в галузі кіберстійкості. Сполучені Штати також застосували багатогранний підхід до цифровізації в національній безпеці, створивши в 2018 році Агентство кібербезпеки і безпеки інфраструктури CISA. Це агентство є центральним координуючим органом для захисту критичної інфраструктури, захисту федеральних мереж і посилення кіберстійкості країни. Розвиваючи партнерські відносини з державними, місцевими, племінними та територіальними органами влади, а також із зацікавленими сторонами з приватного сектору, CISA розробило комплексні рамки для управління ризиками, аналізу загроз та реагування на інциденти. Прийняття таких ініціатив, як Національна система захисту кібербезпеки NCPS і програма безперервної діагностики та пом'якшення наслідків CDM, відображає прагнення Сполучених Штатів використовувати передові технології для виявлення та пом'якшення загроз у режимі реального часу. Роль агентства в просуванні кампаній з підвищення обізнаності громадськості, таких як ініціатива «Зупинись, подумай, підключись», підкреслює важливість залучення громадян до розбудови культури кіберпильності та стійкості.Ініціатива Сінгапуру Розумна нація представляє цілісний підхід до інтеграції цифровізації в державні послуги, визначаючи при цьому цифрову безпеку як наріжний камінь своєї стратегії. Започаткована у 2014 році, ця ініціатива має на меті перетворити Сінгапур на технологічне суспільство, використовуючи аналітику даних, штучний інтелект та Інтернет речей для покращення життя в місті, економічної продуктивності та управління. Ключовим компонентом цієї стратегії є Агентство кібербезпеки Сінгапуру CSA, яке здійснює нагляд за зусиллями країни щодо захисту критично важливої інформаційної інфраструктури та просування освіти з кібербезпеки [10]. Реалізація Національного генерального плану з кібербезпеки та прийняття Закону про кібербезпеку створили надійну правову та інституційну основу для протидії цифровим загрозам. Крім того, використання в Сінгапурі системи Національної цифрової ідентичності NDI забезпечує безпечний і безперешкодний доступ до державних послуг, зміцнюючи довіру і впевненість як серед громадян, так і серед бізнесу.Наведені практичні дослідження ілюструють різноманітні способи інтеграції цифрових технологій у національну безпеку, одночасно вирішуючи унікальні виклики, зумовлені геополітичним і технологічним контекстом кожної країни. Застосовуючи проактивні моделі управління, інвестуючи в передові технології та сприяючи міжсекторальній співпраці, ці країни продемонстрували потенціал цифровізації для посилення національної стійкості, захисту критично важливих активів і забезпечення ефективного державного управління у все більш взаємопов'язаному і складному світі. Уроки, отримані з цього досвіду, слугують цінними орієнтирами для інших країн, які прагнуть орієнтуватися в можливостях і ризиках, пов'язаних з цифровою епохою.

Висновки. Ретроспективний аналіз цифровізації в системі національної безпеки крізь призму державного управління підкреслює трансформаційний вплив технологій на управління безпекою в сучасну епоху. Інтеграція цифрових інструментів і структур у державне управління докорінно змінила спосіб, у який уряди виявляють, реагують і пом'якшують загрози безпеці. Від раннього впровадження обчислювальних систем в обороні до сучасного використання штучного інтелекту і заходів кібербезпеки, діджиталізація послідовно доводить свій потенціал підвищення ефективності, стійкості і адаптивності у вирішенні складних завдань національної безпеки, що постійно ускладнюються.Дослідження підкреслює важливу роль державного управління як сполучної ланки для інтеграції політики, впровадження технологій та міжвідомчої координації. Розвиваючи моделі управління з урахуванням цифрових досягнень, державні адміністратори сприяють безперешкодному впровадженню технологій, які підвищують національну стійкість, захищають критично важливу інфраструктуру та вдосконалюють процеси прийняття рішень. Аналіз конкретних прикладів, зокрема естонської системи електронного урядування, американської стратегії CISA та сінгапурської ініціативи «Розумна нація», показує, як індивідуальні підходи до цифровізації можуть вирішувати унікальні виклики безпеці, водночас сприяючи інноваціям і довірі між зацікавленими сторонами.Можливості для подальших досліджень у цьому напрямі є широкими та багатогранними. Майбутні дослідження можуть глибше зануритися в наслідки нових технологій, таких як квантові обчислення, блокчейн і машинне навчання, для національної безпеки і врядування. Вивчення транскордонних систем цифрового врядування та їхнього впливу на динаміку глобальної безпеки є ще одним напрямком досліджень, особливо у світлі зростаючої геополітичної напруженості і транснаціонального характеру кіберзагроз. Крім того, порівняльні дослідження ефективності цифрових стратегій у різних політичних, економічних і культурних контекстах можуть надати цінну інформацію про передовий досвід і інноваційні рішення.

Список літератури:

1. Ткач М., Ясенко С., Бойко Р., Дриньов Д. Роль і місце систем автоматизації та інформатизації в розвитку потенціалу сектору безпеки та оборони. *Social Development and Security.* 2021. Том 11, № 2. С. 222-230. URL: https://surl.li/aqedau

2. Мосов С. П., Сєлюков, О. В. Космічна розвідка в локальних війнах і збройних конфліктах сучасності. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.* 2019 №3(67) С. 88-93. URL: http://znp-cvsd.nuou.org.ua/article/view/197591/197782

3. ARPANET – The First Internet. *Living Internet.* URL: https://www.livinginternet.com/i/ii_arpanet.htm

4. The Morris Worm: How It Happened and What It Changed. *Cornell Alumni.*URL: https://alumni.cornell.edu/cornellians/morris-worm/

5. Bhardwaj, A., & Kaushik, K. (2022). Predictive analytics-based cybersecurity framework for cloud infrastructure. *International Journal of Cloud Applications and Computing* (IJCAC), 12(1), 1–20. URL: https://www.igi-global.com/gateway/article/297106 .

6. Бігняк П. І., Михальчук В. М. Реформування державного управління: цифровізація. *Інвестиції: практика та досвід*. 2021. № 15. С. 107–113. URL: http://www.investplan.com.ua/?op=1&z=7549&i=15.

7. Bilko, S. Інституційне забезпечення інформаційної безпеки України. 2021. *Економіка і регіон Economics and Region*, (3(82), 36–41. URL: https://journals.nupp.edu.ua/eir/article/view/2361

8. Melnychenko, G., & Belous, S. Innovative development of the region as a component of the general national development strategy. 2020.Scientific notes of Taurida National V.I. Vernadsky University Series: *Economy and Management*, 31(70(1)), 170-174. URL: https://surl.li/qyjrjv

9. Архипова Є.О. Досвід впровадження електронного урядування в Естонії та його імплементація в Україні. *Молодий вчений: Науковий журнал.* 2015. № 11 (26). С. 148-152. URL: https://www.academia.edu/33354754

10. Кіберполітика Сінгапуру: як місто-держава захищається від цифрових загроз. *Аналітичний центр ADASTRA* URL: https://surl.li/spxtmf

Yarovoi T.S. RETROSPECTIVE OF DIGITALISATION IN THE NATIONAL SECURITY SYSTEM THROUGH THE PRISM OF PUBLIC ADMINISTRATION

The article is devoted to the study of the historical trajectory of digitalisation in the national security system with a focus on its evolution through the prism of public administration. The study demonstrates the

transformative role of technology in countering new security threats and maintaining strategic advantages in a rapidly changing global landscape. By tracing key milestones such as the integration of computers into defence systems, the development of real-time command and control mechanisms, and the adoption of advanced cybersecurity measures, the study examines how digital innovations have changed the governance and operational framework of national security.It explores the mechanisms by which state governance has integrated digital tools to enhance national security, with a focus on the creation of cybersecurity agencies, predictive analytics and artificial intelligence. The analysis looks at how countries such as Estonia, the United States and Singapore have implemented effective critical infrastructure protection strategies and established cross-sectoral cooperation. The findings highlight the importance of adaptive policies, innovative technologies, and coordinated efforts to reduce risks from cyber threats and ensure effective governance.Specific challenges and opportunities arising from the digitalisation of national security systems are identified. The study identified issues such as the rapid evolution of cyber threats, the ethical implications of surveillance technologies, and the global digital divide, which require targeted policy responses and international cooperation. The study also highlighted the potential of new technologies, including blockchain and quantum computing, to revolutionise governance and national security. The comparative analysis of different approaches to governance illustrates the diversity of solutions and best practices that can be adapted to different geopolitical and socio-economic contexts.The author substantiates the need for further research at the intersection of digitalisation and public administration, with a focus on the long-term implications of technological progress for national security. The study emphasises the need for innovative governance strategies that balance the benefits of digitalisation with the risks of cyber dependence and data vulnerability.

Key words: *digitalisation, national security, public administration, digitalization of the public administration, ensuring the digitization of public administration, cybersecurity, e-government, crisis management, policy integration, governance models, new technologies, information warfare, geopolitical threats, digital transformation, global security trends.*