УДК 35.078:004.056
DOI https://doi.org/10.32782/TNU-2663-6468/2025.2/04

Вовкотруб С.О.
Київський національний університет імені Тараса Шевченка

ЦИФРОВА БЕЗПЕКА В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ: ЕВОЛЮЦІЯ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У статті розглядаються основні виклики, з якими стикається цифрова безпека в системі державного управління, а також окреслено перспективи її розвитку і вдосконалення. Автор аналізує історичний контекст еволюції цифрових технологій у сфері державного управління та визначає ключові компоненти, які складають основу цифрової безпеки. Особливу увагу приділено дослідженню актуальних кіберзагроз, таких як програм-вимагачі, фішингові атаки, а також проблемам захисту персональних даних. Аналізуються питання відповідності регуляторним вимогам у сфері захисту даних та ризики, пов'язані з цифровізацією державних послуг, які часто є об'єктами кіберзлочинів. Автор пропонує стратегії для посилення цифрової безпеки, зокрема через впровадження принципу «безпеки за дизайном», що передбачає інтеграцію безпекових заходів на ранніх етапах розробки цифрових систем, створення планів реагування на інциденти та застосування новітніх технологій, таких як штучний інтелект та блокчейн. Описано роль цих технологій у підвищенні ефективності захисту інформаційних систем, а також обговорено потенційні етичні виклики та проблеми, які можуть виникнути під час їх впровадження в державні структури. Аналізується також використання архітектури нульової довіри, що передбачає необхідність постійної перевірки доступу до інформаційних систем та компонентів державного управління. Дослідження підкреслює важливість комплексного підходу до забезпечення цифрової безпеки, що включає не лише впровадження сучасних технологій, але й підвищення обізнаності державних службовців щодо актуальних кіберзагроз. Зокрема, значна частина кібератак стає результатом недостатнього навчання персоналу щодо основ кібербезпеки та відсутності культури безпеки на рівні організаційних процесів. Тому автор наголошує на важливості формування у працівників органів державного управління навичок і знань з кібергігієни, а також проведення регулярних тренувань і моделювання атак для підвищення ефективності реакції на інциденти.

Ключові слова: *цифрова безпека, безпека за дизайном, кіберзагрози, захист даних, блокчейн, штучний інтелект.*

Постановка проблеми. Цифрова безпека в системі державного управління стосується практик і технологій, спрямованих на захист чутливих урядових даних та забезпечення цілісності цифрових послуг. В умовах зростаючої залежності державних послуг від цифрових інфраструктур, значення кібербезпеки значно зросло, особливо після численних резонансних кібератак на урядові установи в усьому світі. Забезпечення безпеки цих систем є критичним не лише для підтримки суспільної довіри, але й для захисту персональної інформації громадян та чутливих урядових даних від несанкціонованого доступу та порушень [1; 2].

Ми спостерігаємо, що еволюція цифрової безпеки в державному управлінні тісно пов'язана з ширшим контекстом технологічних досягнень та регуляторних розробок. Принцип «безпеки за дизайном», який передбачає інтеграцію безпекових заходів з самого початку розробки системи, став необхідним для зменшення вразливостей, притаманних цифровим системам. Крім того, відповідність суворим регуляторним вимогам захисту даних, таким як Загальний регламент захисту даних (GDPR), підкреслює правові імперативи, що визначають стратегії цифрової безпеки в межах урядових структур [3; 4].

Незважаючи на прогрес у сфері цифрової безпеки, виклики зберігаються, включаючи ресурсні обмеження, що перешкоджають впровадженню надійних безпекових заходів, зростаючу складність кіберзагроз та потребу в постійному моніторингу і плануванні реагування на інциденти. Органи державної влади стикаються з динамічним кібербезпековим ландшафтом, де загрози на кшталт програм-вимагачів та фішингових атак становлять значні ризики для цілісності даних та суспільної довіри [5; 6].

Інтеграція новітніх технологій, таких як штучний інтелект та блокчейн, пропонує потенційні рішення для посилення безпеки, проте водночас

викликає занепокоєння щодо етичних наслідків та ефективності регуляторних структур [7; 8]. Ми вважаємо, що саме тому дослідження цифрової безпеки в системі державного управління є надзвичайно актуальним в умовах сучасних викликів.

Аналіз останніх досліджень і публікацій. Проблематика цифрової безпеки в державному управлінні активно досліджується науковцями різних галузей. Історичний контекст розвитку державного управління та його інтеграції з цифровими технологіями формувався під впливом значних історичних подій. Кінець XIX століття ознаменував становлення державного управління як окремої академічної дисципліни, що підкреслювало необхідність систематичних підходів до управління в умовах дедалі складніших суспільних процесів [1].

У цей період були запроваджені фундаментальні теорії такими ключовими фігурами як Вудро Вільсон, який у своєму есе 1887 року «Дослідження адміністрації» аргументував необхідність відокремлення політики від адміністрування, заклавши основи для сучасних адміністративних практик [1]. Класична епоха державного управління характеризувалася появою адміністративних теорій, зосереджених на ефективності та ієрархії, з такими вченими як Фредерік Тейлор, який обстоював принципи наукового управління [1; 11].

Значний внесок у дослідження принципу «безпеки за дизайном» зробили сучасні дослідники, які наголошують на важливості інтеграції безпекових заходів на початкових етапах розробки цифрових систем [2; 3]. Питання захисту даних та відповідності регуляторним вимогам, зокрема Загальному регламенту захисту даних (GDPR), детально аналізуються в роботах [4; 5].

Ми відзначаємо, що аналіз кібербезпекових викликів та загроз для державних установ міститься у дослідженнях [6; 7], де особлива увага приділяється проблемам атак програм-вимагачів та фішингу. Стратегії посилення цифрової безпеки, включаючи планування реагування на інциденти та впровадження архітектури нульової довіри, висвітлюються в роботах [9; 10; 12; 13].

Серед сучасних науковців, які у тій чи іншій мірі, присвятили увагу дослідженню проблематики цифрової безпеки в системі державного управління доцільно назвати наступних: Є.П. Бабалик, О.Є. Бухтатий, О.О. Григор, О.В.Карпенко, А.М. Митко, П.С. Клімушин, Р.А. Коваль, В.О. Коновал, Н.Б. Новицька, О.В. Павлишин та ін.

Однак, на нашу думку, питання комплексного підходу до цифрової безпеки в державному управлінні з урахуванням сучасних технологічних тенденцій залишається недостатньо дослідженим, що обґрунтовує необхідність нашого дослідження.

Постановка завдання. Метою нашого дослідження є комплексний аналіз та характеристика ключових викликів та перспектив цифрової безпеки в системі державного управління в умовах динамічного технологічного розвитку.

Виклад основного матеріалу. Еволюція державного управління та його інтеграція з цифровими технологіями формувалися під впливом значних історичних перетворень [1]. На нашу думку, саме наприкінці XIX століття було закладено підвалини для формування сучасних підходів до державного управління. У цей період відбувалася інституціоналізація бюрократії, впроваджувалися механізми раціонального управління та стандартизовані адміністративні процедури. Значний вплив на подальшу модернізацію державного управління справили індустріальна революція, розвиток правових концепцій публічного адміністрування та зростання потреби у впровадженні ефективних управлінських практик.

Класична ера державного управління характеризувалася появою адміністративних теорій, зосереджених на ефективності та ієрархії, з ученими на кшталт Фредеріка Тейлора, який обґрунтовував принципи наукового управління [1; 11]. Цей період трактував громадян переважно як пасивних клієнтів державних послуг, відображаючи бюрократичний підхід до адміністрування [1]. Ми вважаємо, що такий підхід, хоча й забезпечував певну стабільність та передбачуваність, не відповідає сучасним вимогам до гнучкості та відкритості державного управління.

У середині XX століття ера мобілізації та реформ принесла значні зміни в державне управління, особливо у відповідь на соціально-економічні виклики, такі як Велика депресія та наслідки Другої світової війни. Цей період характеризувався розширенням державних програм і бюрократії, що призвело до зрушення в бік більш партисипативних моделей управління. Запровадження систем соціального забезпечення в Європі та США свідчило про зростаюче визнання ролі державного управління у вирішенні соціальних потреб та сприянні економічній стабільності [1].

З настанням цифрової ери наприкінці XX – на початку XXI століть державне управління зазнало глибокої трансформації через цифровізацію послуг. Цей перехід приніс як підвищення ефективності, так і нові вразливості, що зумовило необхідність зосередження уваги на кібербезпеці

та захисті даних. Принцип «безпеки за дизайном» виник як життєво важлива концепція, що передбачає інтеграцію безпекових заходів від самого початку розробки цифрових систем для захисту від кіберзагроз та забезпечення довіри до державного управління [2].

На нашу думку, історичний контекст державного управління відображає постійну напругу між прагненням до ефективності та необхідністю забезпечення підзвітності та залучення громадян – динаміку, яка залишається критичною в сучасному ландшафті цифрового управління [2].

Цифрова безпека в системі державного управління охоплює різноманітні стратегії та практики, спрямовані на захист даних та підтримку цілісності цифрових послуг. Ми переконані, що з огляду на зростаючу залежність державних послуг від цифрових технологій, забезпечення безпеки цих систем стало першочерговим для підтримки суспільної довіри та захисту персональної інформації.

Принцип «безпеки за дизайном» є фундаментальним для ефективної цифрової безпеки. Цей підхід передбачає інтеграцію безпекових заходів у розробку цифрових систем з самого початку, а не як додаткове міркування. Ключові елементи включають проведення ретельних оцінок безпекових ризиків, впровадження практик безпечного кодування та реалізацію надійних механізмів контролю доступу. Регулярне тестування безпеки протягом усього життєвого циклу розробки додатково підвищує стійкість проти потенційних порушень [2; 3].

У галузі державного управління захист персональних даних є як юридичною вимогою, так і необхідністю для підтримки суспільної довіри. Дотримання таких регуляторних вимог, як Загальний регламент захисту даних (GDPR), передбачає суворі правила обробки даних. Це включає впровадження таких заходів, як шифрування даних, яке захищає інформацію як під час передачі, так і в стані спокою, а також забезпечення прозорості щодо використання даних, щоб розширити можливості користувачів контролювати свою інформацію [4; 5].

Ефективний план реагування на інциденти є критично важливим для протидії кіберзагрозам. Цей план окреслює протоколи виявлення, аналізу та реагування на безпекові інциденти, включаючи чітко визначені ролі та відповідальність. Регулярні тренування та огляди після інцидентів є важливими для постійного вдосконалення можливостей реагування та мінімізації майбутніх ризиків [3].

Постійний моніторинг цифрових систем щодо підозрілої активності є життєво важливим для швидкого виявлення та пом'якшення загроз. Це включає впровадження систем виявлення вторгнень, які попереджають адміністраторів про потенційні порушення. Регулярні аудити забезпечують відповідність стандартам безпеки та надають інформацію про сфери, які потребують удосконалення [5].

Впровадження новітніх технологій, таких як штучний інтелект (ШІ), машинне навчання (ML) та блокчейн, трансформує стратегії цифрової безпеки в державному управлінні. Ми вважаємо, що ці технології можуть посилити можливості виявлення загроз та реагування на них, захистити чутливі дані та покращити загальну безпекову позицію цифрових інфраструктур. Крім того, прийняття таких концепцій як архітектура нульової довіри, яка передбачає, що загрози можуть походити як зовні, так і зсередини організації, додатково зміцнює безпекові заходи [3].

Операційна безпека (OPSEC) відіграє вирішальну роль у захисті інформації під час повсякденних бізнес-операцій. Навчання працівників розпізнавати кіберзагрози, такі як фішинг та атаки соціальної інженерії, та реагувати на них, є необхідним для формування культури обізнаності щодо кібербезпеки. Впровадження суворих механізмів контролю доступу та моніторинг активності користувачів може допомогти пом'якшити інсайдерські загрози, які становлять значні ризики для цілісності та конфіденційності даних [5].

Цифрова безпека в державному управлінні стикається з численними викликами, що випливають із швидкої цифровізації послуг. Хоча цей перехід пропонує підвищену ефективність та покращений доступ до послуг, він одночасно створює значні ризики захисту даних та безпеки, які мають бути всебічно вирішені для підтримки суспільної довіри в ці системи [2; 4].

Оскільки системи державного управління стають все більш залежними від цифрових технологій, вони стають все більш вразливими до кібератак. Ми вважаємо, що інтеграція принципів «безпеки за дизайном» є необхідною, вбудовуючи безпекові заходи на початкових етапах розробки системи для мінімізації вразливостей [2]. Водночас значна частина державних установ функціонує в умовах обмежених ресурсів, що створює перешкоди для впровадження комплексних заходів захисту інформаційних систем [3]. Недостатнє фінансування, нестача висококваліфікованих фахівців у сфері кібербезпеки та складність

адаптації регуляторних вимог у цифровому середовищі можуть робити державні інформаційні системи вразливими до атак.

Ландшафт кіберзагроз постійно еволюціонує, причому атаки програм-вимагачів прогнозуються як найзначніша загроза кібербезпеці для бізнесу до 2024 року. Ці атаки часто є складними і використовують передові технології, включаючи штучний інтелект, для обходу традиційних безпекових заходів [6]. Інші поширені загрози включають фішинг, спрямований на маніпулювання особами для розголошення чутливої інформації, та атаки типу «відмова в обслуговуванні», які порушують критичну інфраструктуру [7]. Зростаюча частота таких атак підкреслила нагальну потребу в ефективних стратегіях кібербезпеки в системах державного управління.

Захист персональних даних у системах цифрового адміністрування є основним викликом. Державне управління повинно впроваджувати постійний моніторинг та оновлення безпекових заходів для захисту чутливої інформації від порушень [4]. Ризики, пов'язані з неадекватним захистом даних, можуть призвести до значних наслідків, включаючи ерозію суспільної довіри та потенційні правові наслідки через недотримання регуляторних вимог захисту даних [2].

На нашу думку, прийняття новітніх технологій, таких як блокчейн, квантові обчислення та розширене спільне використання розвідки про загрози, є важливим для посилення державної кібербезпеки. Ці технології пропонують інноваційні рішення для захисту чутливих даних та покращення можливостей виявлення загроз [3]. Однак успішна інтеграція таких технологій вимагає подолання існуючих ресурсних обмежень та сприяння співпраці між державним і приватним секторами для зміцнення заходів кібербезпеки [8].

Планування реагування на інциденти є фундаментальним аспектом комплексної стратегії кібербезпеки у державному управлінні. Це забезпечує швидке та ефективне реагування організацій на безпекові інциденти, мінімізуючи шкоду та відновлюючи послуги якомога швидше. План реагування на інциденти зазвичай окреслює процедури виявлення, аналізу, стримування, ліквідації та відновлення після кіберінцидентів. Ключові елементи включають чітко визначені ролі та відповідальність, стратегії комунікації та процедури ескалації [3].

Для ефективного забезпечення цифрових трансформацій уряду необхідний стратегічний та всебічний підхід до кібербезпеки. Ми переконані, що прийняття підходу «безпеки за дизайном» означає інтеграцію безпекових заходів у процес розробки цифрових систем з самого початку, а не як додаткове міркування. Ця проактивна стратегія охоплює ретельні оцінки безпекових ризиків під час планування, практики безпечного кодування, надійні механізми контролю доступу та регулярне тестування безпеки протягом усього життєвого циклу розробки [3; 2].

Впровадження архітектури нульової довіри є ще однією критично важливою стратегією. Ця модель припускає, що загрози можуть існувати як всередині, так і поза мережею, таким чином вимагаючи суворої перевірки кожного користувача та пристрою, які намагаються отримати доступ до ресурсів. Прийняття принципів нульової довіри дозволяє державним організаціям краще захищати чутливі дані та зменшувати потенційний вплив порушень [3].

Інтеграція новітніх технологій, таких як штучний інтелект, машинне навчання та блокчейн, відіграє ключову роль у посиленні державної кібербезпеки. Ці технології пропонують інноваційні рішення для захисту чутливих даних, забезпечення цілісності транзакцій та покращення загальних можливостей виявлення та реагування на загрози [3; 4].

Формування культури обізнаності щодо кібербезпеки серед працівників є необхідним для зменшення ризиків, пов'язаних з людською помилкою [9]. Значна частина кібератак стає можливою саме через недоліки у поведінці користувачів, недостатню цифрову грамотність та нехтування елементарними принципами захисту інформації. У зв'язку з цим особливого значення набуває розробка та впровадження системних навчальних програм, спрямованих на підвищення обізнаності працівників щодо актуальних кіберзагроз, включаючи методи соціальної інженерії, спроби фішингу та безпечне поводження з конфіденційною інформацією.

Ефективні освітні ініціативи у сфері кібербезпеки мають ґрунтуватися на комплексному підході, що передбачає регулярне оновлення навчальних матеріалів, інтерактивні тренінги, моделювання реальних сценаріїв атак, а також використання тестових ситуацій для перевірки рівня підготовки персоналу. Регулярні сесії з підвищення кібероб'єднаності можуть значно посилити ефективність захисних заходів, трансформуючи працівників державних установ у першу лінію оборони проти кібератак.

Співпраця з партнерами з приватного сектору та міжнародними організаціями посилює обмін

знаннями та об'єднання ресурсів, що призводить до більш ефективних безпекових заходів. Крім того, регулярні оцінки ризиків кібербезпеки та комплексні плани реагування на інциденти, узгоджені з федеральними стандартами, гарантують, що державні організації готові до нових загроз і можуть ефективно реагувати на інциденти, коли вони виникають [10; 12; 13].

Дослідження кейсів дозволяє нам краще зрозуміти практичне застосування принципів цифрової безпеки. Цікавим прикладом є кейс, проведений на північному сході Англії, який вивчав спільні зусилля громади, що використовує цифрову платформу обміну інформацією для навігації викликів, спричинених змінами в політиці соціального добробуту. Це дослідження підкреслило, як місцеві сутності могли колективно реагувати на соціальний тиск, одночасно вирішуючи ширші проблеми безпеки [15].

Ми звернули увагу на тенденцію урядових підходів пріоритезувати технологічну безпеку над безпекою окремих громадян, виявляючи критичний розрив у поточних структурах кібербезпеки. На нашу думку, дослідження обґрунтовано виступає за більш інклюзивні архітектури кібербезпеки, які враховують добробут та безпеку членів громади поряд з технологічними заходами безпеки [15].

Ландшафт судових позовів щодо порушення даних у Сполучених Штатах значно впливає на правові прецеденти, зокрема рішення Верховного суду США у справі TransUnion проти Ramirez у 2021 році. Цей випадок встановив жорсткі вимоги для позивачів демонструвати правовий статус у федеральному суді при переслідуванні претензій, пов'язаних з порушеннями даних. Рішення підкреслило, що сам ризик майбутньої шкоди недостатній для встановлення конкретної шкоди, що є критичним міркуванням для осіб, чиї дані були скомпрометовані, але ще не використані неправомірно [16].

На нашу думку, цей випадок служить ключовою точкою відліку для розуміння правових викликів, з якими стикаються позивачі в діях щодо порушення даних, та підкреслює важливість правових структур у формуванні дискурсу навколо цифрової безпеки [16].

У грудні 2023 року Федеральна комісія зв'язку (FCC) впровадила нові модифікації правил повідомлення про порушення даних для провайдерів телекомунікацій, включаючи тих, що пропонують взаємопов'язані голосові послуги через Інтернет-протокол (VoIP) та телекомунікаційні релейні послуги (TRS). Ці модифікації розширили визначення особисто ідентифікованої інформації, яка повинна бути повідомлена у випадку порушення, та встановили нові зобов'язання щодо повідомлення FCC [16].

Ми вважаємо, що ця регуляторна зміна ілюструє еволюційний ландшафт цифрової безпеки в державному управлінні, підкреслюючи необхідність проактивних заходів у захисті чутливої інформації в різних секторах [16].

Дослідження впровадження систем цифрового адміністрування підкреслює необхідність вбудовування безпекових протоколів у дизайн цих систем. Принцип «безпеки за дизайном» забезпечує інтеграцію безпекових заходів з самого початку, зменшуючи вразливості та підвищуючи стійкість цифрової інфраструктури. Цей підхід є необхідним для суспільної довіри та ефективного функціонування урядових послуг, які все більше покладаються на цифрові рішення [2; 17].

Ландшафт цифрової безпеки в державному управлінні готовий до значної еволюції в найближчі роки, зумовлений прогресом у технологіях та посиленим регуляторним контролем. Оскільки організації продовжують адаптуватися до нових дата-інтенсивних технологій, ми прогнозуємо, що тенденції, такі як зміщення від відстеження на стороні браузера до технологій відстеження на стороні сервера, зміцняться до 2026 року, частково через поточні зусилля з узгодження з законами про приватність [18].

Ми очікуємо, що 2025 рік побачить продовження посиленої регуляторної та правозастосовної діяльності з боку федеральних та державних агенцій в США. Це посилення контролю є значною мірою відповіддю на швидкі досягнення в технологіях, таких як штучний інтелект (ШІ) та Інтернет речей (IoT), а також на постійні кіберзагрози, що створюються зловмисниками [16]. За відсутності комплексного федерального законодавства, агенції, ймовірно, будуть переслідувати агресивні правозастосовні дії проти організацій, які не дотримуються еволюційних стандартів приватності та захисту даних [16].

На нашу думку, інтеграція новітніх технологій в операції державного сектору перебудує динаміку робочого місця та процеси прийняття рішень. Прийняття складних технологій, включаючи ШІ та блокчейн, очікувано посилить прозорість, ефективність та громадянську залученість. Однак, це також викликає занепокоєння щодо потенційного заміщення робочих місць та етичних наслідків автоматизованого прийняття рішень [19; 20].

Ми очікуємо, що блокчейн-технологія набуває все більшого визнання за її потенціал покращити безпеку та прозорість систем державного управління. Її децентралізована та незмінна природа представляє можливості для покращеного управління даними, безпечних систем голосування та прозорих процесів державних закупівель [20; 22; 23]. Використовуючи блокчейн, державні агенції можуть посилити довіру до управління та спростити операції, хоча прийняття цієї технології все ще на ранніх стадіях і може стикатися з регуляторними викликами [23].

Штучний інтелект та предиктивна аналітика, на нашу думку, відіграватимуть життєво важливу роль у виявленні тенденцій та потенційних ризиків управління, тим самим дозволяючи державним адміністраціям проактивно вирішувати проблеми до їхньої ескалації. Автоматизовані аудити та реалізація політик у реальному часі спростять операції та зменшать потенціал для людської помилки [22]. Оскільки агенції державного сектору все більше покладаються на аналітику даних, захист чутливої інформації залишиться першочерговим, вимагаючи надійних структур захисту даних [4].

Таким чином, можемо резюмувати, що до основних викликів цифрової безпеки в державному управлінні належать наступні: 1) зростаюча вразливість державних систем до кібератак – урядові установи дедалі більше покладаються на цифрові платформи та ІТ-інфраструктури, що робить їх привабливими цілями для кіберзлочинців. Злам урядових порталів, систем електронного документообігу чи реєстрів може призвести до масштабних витоків інформації й порушення суспільної довіри; 2) проблема захисту персональних даних – зростає суспільне занепокоєння через імовірність витоків або нецільового використання персональних даних громадян. Недотримання норм захисту інформації підриває довіру до державних інституцій. Активне впровадження штучного інтелекту, блокчейну, хмарних обчислень створює нові можливості для розвитку, але водночас з'являються додаткові ризики й труднощі забезпечення захисту таких рішень; 3) брак комплексного підходу й людський фактор – недостатня кіберграмотність персоналу, фрагментованість заходів безпеки та відсутність внутрішньої "культури кіберобізнаності" робить навіть сучасно захищені системи вразливими. Працівники можуть випадково стати "слабкою ланкою", піддаючись фішинговим листам або розкриваючи облікові дані. Організаційна культура, де безпека сприймається як формальність, а не як пріоритет, суттєво знижує ефективність навіть добре розроблених політик. Відсутність узгодженої стратегії співпраці між різними департаментами чи відомствами створює прогалини у захисному периметрі.

Щодо стратегічних рекомендацій для посилення цифрової безпеки, то, на основі здійсненого нами аналізу, до них віднесено такі: 1) планування реагування на інциденти – розроблення та регулярне оновлення комплексного плану дій у випадку кіберінцидентів для оперативного виявлення, стримування та ліквідації наслідків. А саме доцільним є створення спеціалізованих груп із чітко визначеними ролями та повноваженнями, проведення регулярних навчальних тренувань і моделювання можливих атак з метою перевірки готовність персоналу й технічних систем; 2) впровадження підходу "безпеки за дизайном" – інтеграція заходів безпеки ще на початкових стадіях проєктування й розробки цифрових систем та послуг. Це передбачає здійснення попереднього аналізу ризиків перед запуском будь-якого цифрового проєкту, регулярне тестування безпеки на кожному етапі створення продукту, використання архітектурних рішень, орієнтованих на мінімізацію вразливостей (принцип найменших привілеїв, шифрування за замовчуванням, сегментація мережі); 3) архітектура нульової довіри – модель, яка не надає автоматичної довіри жодному елементу системи (користувачам, пристроям або мережам), навіть внутрішнім. Кожен запит на доступ вимагає перевірки та автентифікації. Постійний моніторинг користувацьких сесій і застосування політик доступу, що динамічно змінюються відповідно до ризик-профілю; 4) формування культури кібербезпекової обізнаності – створення середовища, де всі працівники органів влади усвідомлюють важливість захисту інформаційних ресурсів та вміють реагувати на базові кіберзагрози. Це передбачає проведення регулярних навчальних сесій з основ кібергігієни (розпізнавання фішингових листів, безпечне зберігання паролів, правильна робота з конфіденційними документами), а також моделювання сценаріїв фішинг-атак або соціальної інженерії для практичного відпрацювання навичок.

Висновки. У результаті проведеного дослідження ми дійшли висновку, що цифрова безпека в системі державного управління є багатогранною та еволюціонуючою сферою, яка відіграє критичну роль у забезпеченні ефективності та надійності урядових послуг у все більш цифровому світі. Історичний розвиток державного управ-

ління демонструє поступову трансформацію від бюрократичних моделей до цифрових систем, що вимагає інтеграції безпекових підходів на всіх етапах проектування та впровадження.

На основі аналізу кейсів ми виявили тенденцію урядових підходів пріоритезувати технологічну безпеку над безпекою окремих громадян, що вказує на необхідність розробки більш інклюзивних архітектур кібербезпеки. Значущими також є правові аспекти цифрової безпеки, що формують дискурс навколо захисту даних та відповідальності за їх порушення.

Майбутні тенденції цифрової безпеки в державному управлінні, на нашу думку, будуть пов'язані з посиленою регуляторною діяльністю, інтеграцією таких технологій як блокчейн та штучний інтелект, трансформацією робочих процесів та розвитком предиктивної аналітики. Ці тенденції формуватимуть ландшафт цифрової безпеки та вимагатимуть адаптації стратегій захисту.

Ми переконані, що ефективна цифрова безпека в державному управлінні вимагає балансу між технологічними рішеннями, нормативно-правовим регулюванням та розвитком людського капіталу. Лише комплексний підхід, що враховує всі аспекти безпеки, дозволить забезпечити надійний захист цифрових систем та підтримати суспільну довіру до державних інституцій.

Список літератури:

1. Public Administration Institute. The Evolution and Current Status of Public Administration as a Discipline. Public Administration Notes by PubAdmin.Institute: вебсайт. 2023. URL: https://surl.li/oumath (дата звернення: 16.01.2024).

2. World Policy Hub. The Evolution of Public Administration: Key Phases and Stages: вебсайт. 2023. URL: https://surl.lu/xaueed (дата звернення: 16.01.2024).

3. Podoba R. Public Administration Faces Increasing Cybersecurity Challenges The digitalization of public services. LinkedIn: вебсайт. 2024. URL: https://surl.li/itoinq (дата звернення: 16.01.2024).

4. Best C. Cybersecurity Best Practices for Securing Government Digital Transformation. Quadrant Four: вебсайт. 2024. URL: https://surl.li/vgwofw (дата звернення: 16.01.2024).

5. CCNet. Data-Protection & Security in Digital Administration Systems. CCNet – Blog: вебсайт. 2024. URL: https://surl.li/xlvubo (дата звернення: 16.01.2024).

6. Slonopas A. What Is Cybersecurity? Understanding Its Basic Components. Apus.edu: вебсайт. 2024. URL: https://surl.lu/rmqiiq (дата звернення: 16.01.2024).

7. SentinelOne. Top 7 Cyber Attacks in the United States: вебсайт. 2024. URL: https://surl.li/nzsgjr (дата звернення: 16.01.2024).

8. Woodland E. 10 Cyber Security Best Practices for the Public Sector. Govnet.co.uk: вебсайт. 2024. DOI: https://doi.org/10097256717/module_40176343970_blog-footer.

9. Carpenter S. 5 cybersecurity issues that the public sector faces and how to protect it. Open Access Government: вебсайт. 2021. URL: https://surl.li/ppurcf (дата звернення: 16.01.2024).

10. UpGuard. Guarding Governance: Cybersecurity in the Public Sector: вебсайт. 2024. URL: https://www.upguard.com/blog/cybersecurity-in-the-public-sector (дата звернення: 16.01.2024).

11. Tenable. CISA Releases FOCAL Plan to Help Federal Agencies Reduce Cyber Risk: вебсайт. 2024. URL: https://surl.li/diviik (дата звернення: 16.01.2024).

12. Clomera A. 15 Most Common Cyber Attacks for Federal Agencies. IPKeys: вебсайт. 2024. URL: https://ipkeys.com/blog/types-of-cyber-attacks/ (дата звернення: 16.01.2024).

13. Belderbos H. Protecting the public sector against cyberattacks. Open Access Government: вебсайт. 2024. URL: https://surl.li/uatyod (дата звернення: 16.01.2024).

14. Public Sector Experts. Crisis Management: Lessons from the Public Sector – Navigating Turbulent Times: вебсайт. 2024. URL: https://surl.li/kzxewn (дата звернення: 16.01.2024).

15. SE A. Cybersecurity Challenges in the Public Sector: Safeguarding Digital Infrastructures and Citizen Data. Academia.edu: вебсайт. 2024. URL: https://surl.li/xsvnra (дата звернення: 16.01.2024).

16. Manfredi R. U.S. Cybersecurity and Data Privacy Review and Outlook – 2024. Gibson Dunn: вебсайт. 2024. URL: https://surli.cc/odhzae (дата звернення: 16.01.2024).

17. SoloWay. Government Digital Transformation: Benefits And Challenges In 2024: вебсайт. 2023. URL: https://soloway.tech/blog/digital-transformation-in-government/ (дата звернення: 16.01.2024).

18. Ramos G. A. 5 Trends to Watch: 2024 U.S. Data Privacy & Cybersecurity. Natlawreview.com: вебсайт. 2024. URL: https://surl.li/wnybvk (дата звернення: 16.01.2024).

19. UC Berkeley Labor Center. Technology in the public sector and the future of government work: вебсайт. 2023. URL: https://surl.gd/avwqij (дата звернення: 16.01.2024).

20. Cole J. Global Case Studies: Blockchain Initiatives in the Public Sector. BlockApps Inc: вебсайт. 2024. URL: https://blockapps.net/blog/global-case-studies-blockchain-initiatives-in-the-public-sector/ (дата звернення: 16.01.2024).

21. Governancepedia. Technology's Impact on Governance: The Age of Digital Oversight: вебсайт. 2024. URL: https://surl.gd/tkdcmn (дата звернення: 16.01.2024).

22. Treiblmaier H., Sillaber C. A Case Study of Blockchain-Induced Digital Transformation in the Public Sector. Progress in IS. 2020. P. 227–244. URL: https://surl.lu/himjlw (дата звернення: 16.01.2024).

Vovkotrub S.O. DIGITAL SECURITY IN THE PUBLIC ADMINISTRATION SYSTEM: EVOLUTION, CHALLENGES AND DEVELOPMENT PROSPECTS

The article discusses the main challenges faced by digital security in the public administration system and outlines the prospects for its development and improvement. The author analyzes the historical context of the evolution of digital technologies in the field of public administration and identifies the key components that form the foundation of digital security. Special attention is given to the examination of current cyber threats, such as ransomware attacks, phishing, and issues related to the protection of personal data. The article also addresses compliance with regulatory requirements in data protection and the risks associated with the digitalization of public services, which are often targets of cybercrimes. The author proposes strategies for enhancing digital security, particularly through the implementation of the «security by design» principle, which involves integrating security measures at the early stages of digital system development, creating incident response plans, and applying cutting-edge technologies such as artificial intelligence and blockchain. The role of these technologies in improving the effectiveness of information system protection is described, as well as the potential ethical challenges and issues that may arise during their implementation in public institutions. The article also examines the use of a zero-trust architecture, which requires constant verification of access to information systems and components of public administration. The study emphasizes the importance of a comprehensive approach to ensuring digital security, which includes not only the implementation of modern technologies but also raising the awareness of public servants about current cyber threats. In particular, a significant portion of cyberattacks results from insufficient training of personnel on the fundamentals of cybersecurity and the lack of a security culture at the organizational level. Therefore, the author stresses the importance of developing skills and knowledge of cyber hygiene among public administration employees, as well as conducting regular training sessions and simulating attacks to enhance the effectiveness of incident response.

Key words: *digital security, security by design, cyber threats, data protection, blockchain, artificial intelligence.*