УДК 35:005.591(477)

О. П. Попов,
аспірант кафедри менеджменту та бізнес-адміністрування,
Прикарпатський національний університет імені Василя Стефаника
ORCID ID: https://orcid.org/0000-0003-4066-4349

DOI: 10.32702/2306-6814.2024.16.309

БЕЗПЕКОВІ АСПЕКТИ ЦИФРОВОЇ ВЗАЄМОДІЇ У СИСТЕМІ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ В УКРАЇНІ

O. Popov,
Postgraduate student of the Department of Management and Business Administration,
Vasyl Stefanyk Precarpathian National University

SECURITY ASPECTS OF DIGITAL INTERACTION IN THE SYSTEM OF PUBLIC AUTHORITIES IN UKRAINE

У статті досліджуються безпекові аспекти цифрової взаємодії у системі органів публічної влади в Україні. Наголошуючи на важливості інтеграції сучасних технологій для підвищення ефективності та прозорості державних послуг, підкреслено важливі виклики безпеки, які супроводжують процеси трансформаційних змін. Дослідження визначає законодавчі прогалини у сфері кібербезпеки, що ускладнюють ефективну боротьбу з кіберзагрозами. Запропоновано гармонізувати національне законодавство з міжнародними стандартами та впровадити єдині національні стандарти кібербезпеки для критичної інфраструктури. Підкреслено критичну потребу фінансових інвестицій у кібербезпеку. Передові технології, такі як штучний інтелект і машинне навчання, окреслюються як важливі інструменти для боротьби з кіберзлочинністю, що потребує значної фінансової підтримки для впровадження та функціонування. Закцентовано увагу на необхідності комплексного підходу, включаючи національну сертифікацію критичної інфраструктури та посилені інформаційні кампанії з підвищення обізнаності громадськості.

The article explores the security aspects of digital transformation in public administration in Ukraine. Highlighting the significance of integrating modern technologies to enhance efficiency and transparency of government services, the author emphasizes the critical security challenges that accompany digital interaction. The study identifies legislative gaps in cybersecurity, hindering effective responses to cyber threats. It proposes harmonizing national legislation with international standards and implementing unified national cybersecurity standards for critical infrastructure. Additionally, the article stresses the necessity of creating a coordinated system and increasing cybersecurity funding.

The analysis draws attention to the insufficient detail in existing cybersecurity laws, which often lack specific criteria and procedures for threat assessment and response. The absence of clear standards leads to inconsistent approaches across various organizations, complicating coordination and cooperation. Recent legislative initiatives, while important, still fall short in providing detailed response mechanisms and criteria for evaluating system effectiveness.

Addressing the broader issue of limited funding and resources, the article underscores the critical need for financial investment in cybersecurity. Advanced technologies, such as artificial intelligence and machine learning, are highlighted as essential tools for combating cybercrime, requiring substantial financial support for implementation and operation.

The article also discusses the significant shortage of qualified cybersecurity professionals, a challenge exacerbated by inadequate funding and training opportunities. The rapid evolution of cyber threats necessitates continuous education and skill development, which current budget constraints do not sufficiently support. The authors advocate for a comprehensive approach, including national certification for critical infrastructure and enhanced public awareness campaigns.

In conclusion, the article calls for a coordinated national effort to strengthen cybersecurity through legislative improvements, increased funding, and better resource allocation. By addressing these challenges, Ukraine can develop a more robust and effective cybersecurity system to meet contemporary threats and safeguard public administration processes.

Ключові слова: цифрова взаємодія органів публічної влади, безпекові аспекти, критична інфраструктура, інформаційні системи, кібербезпека, кіберзагрози.

Key words: digital interaction of public authorities, security aspects, critical infrastructure, information systems, cyber security, cyber threats.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Згідно з дослідженнями Міжнародного центру цифрової конкуренції — Digital Report 2022, десятки європейських країн оцифрували свої органи управління [1]. Лідерами цього процесу є Фінляндія, Данія, Швеція, а також Естонія та Мальта. У сучасному світі громадяни та компанії не можуть уявити повсякденне життя без мобільних телефонів, ноутбуків, Інтернету, електронного підпису, численних додатків та програмного забезпечення, а також безготівкових платежів, що викликає потребу у впровадженні відповідних ефективних рішень [2]. Цифровізація процесів у публічному управлінні наразі обмежується перетворенням паперових документів у цифрові формати. Це створює технічну та організаційну основу для подальшої цифрової трансформації, але не є достатнім для значних покращень. Неузгодженість і локальне використання різних центрів обробки даних та додатків призводять до складної та незручної взаємодії органів публічної влади зі споживачами послуг. Все це свідчить про те, що цифровізація усіх процесів стає нагальною потребою діяльності органів публічної влади, що вимагає забезпечення високого рівня безпеки. Впровадження новітніх технологій у публічному секторі дозволяє підвищити ефективність і прозорість надання державних послуг, полегшити доступ громадян до інформації, а також забезпечити більш оперативне реагування на запити суспільства. Однак, разом із численними можливостями, цифрова взаємодія в системі органів публічної влади України несе і низку серйозних безпекових викликів.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

В наукових працях як вітчизняних, так і зарубіжних фахівців розглядається широкий спектр питань, пов'язаних із безпековими аспектами цифрової взаємодії органів публічної влади. Зокрема, останні дослідження акцентують увагу на необхідності інтеграції новітніх технологій у публічне управління для підвищення ефективності, прозорості та підзвітності публічних інституцій [3].

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Формулювання цілей статті (постановка завдання) полягає у визначенні безпекових аспектів цифрової трансформації органів публічної влади в Україні, аналізу актуальних викликів і ризиків, розробки рекомендацій з урахуванням міжнародного досвіду та передових технологій.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Технологічний прогрес значно збільшує необхідність забезпечення високого рівня безпеки у публічному просторі. Інновації стали невід'ємною частиною публічних установ, використовуючи потенціал висококваліфікованих працівників. Застосування додатків, доповнень та інтелектуальної автоматизації процесів значно зменшує прогалини у цифровізації, забезпечуючи відповідний рівень безпеки.

Однак, не зважаючи на ці зусилля, регулярні повідомлення ЗМІ про хакерські атаки на органи публічної влади підривають довіру громадян до безпеки даних. Для вирішення цієї проблеми необхідно впроваджувати комплексні концепції безпеки для державних інформаційних систем, бізнесу та громадян. Для забезпечення високого рівня безпеки та ефективності функціонування, органи публічної влади мають поступово інтегрувати інноваційні технології. Поступове впровадження цифрових рішень сприятиме значному прогресу у зміцненні безпеки та підвищенні ефективності публічного управління.

Недостатня деталізація положень у законодавстві з кібербезпеки є серйозним викликом, який значно ускладнює його ефективне впровадження. Законодавство часто обмежується загальними фразами, без конкретизації та чітких положень, що робить його виконання складним та непередбачуваним. Наприклад, відсутність чітких критеріїв і процедур для оцінки кіберзагроз та реагування на них створює значні труднощі для органів публічної влади та приватних компаній. Закон України "Про кібербезпеку" хоча й встановлює загальні засади забезпечення кібербезпеки, проте не містить детальних процедур та алгоритмів дій у разі виявлення кіберінцидентів. Окрім того, має місце відсутність стандартів для оцінки кіберзагроз, оскільки закони та підзаконні акти часто не містять конкретних стандартів і методик для оцінки кіберзагроз. Наприклад, чинний Закон України 1994 року "Про захист інформації в інформаційно-телекомунікаційних системах" [4] визначає загальні вимоги до захисту інформації, але не містить чітких критеріїв для оцінки рівня захищеності систем. Це призводить до різних підходів у різних органах публічної влади, що ускладнює координацію та співпрацю між ними. У цьому зв'язку виникає потреба розробки та впровадження єдиних національних стандартів, таких як ДСТУ ISO/IEC 27001:2017 "Системи управління інформаційною безпекою", що будуть визначати чіткі критерії оцінки кіберзагроз.

Однак варто також зазначити, що у 2020 році ухвалено Закон України "Про внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації". Хоча закон вводить поняття "комплексної системи захисту інформації", він не надає чітких критеріїв для оцінки того, наскільки система відповідає цим вимогам. Потрібні більш деталізовані стандарти та методики оцінки. При цьому видається не зовсім зрозуміло, як буде організована і проводитися державна експертиза, які саме критерії будуть використовуватися для оцінки систем, які органи будуть відповідальні за проведення експертизи. Хоча закон передбачає можливість обробки деяких категорій інформації без повної комплексної системи захисту, вимоги до таких систем можуть бути недостатньо чіткими. Окрім того, впровадження нових вимог потребує часу та ресурсів, що зобов'язує розробити відповідні підзаконні акти та провести інформаційно-роз'яснювальну роботу серед органів влади та суб'єктів господарювання [5].

Нормативно-правові акти не завжди регламентують чіткі процедури реагування на кіберінциденти. Постанова КМУ "Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки" від 23 грудня 2020 року № 1295 закладає фундамент для створення та функціонування системи виявлення вразливостей і реагування на кіберінциденти в Україні; визначає Державний центр кіберзахисту Державного агентства спеціального зв'язку та захисту інформації як відповідального за функціонування системи; передбачає встановлення спеціального обладнання на об'єктах критичної інфраструктури для збору даних про кіберзагрози; визначає механізми взаємодії між різними суб'єктами кібербезпеки. Це свідчить про системний підхід до забезпечення кібербезпеки; централізацію управління системою, встановлення чітких відповідальностей. Однак, на нашу думку, вона не позбавлена недоліків, оскільки має місце недостатня деталізація процедур реагування на кіберінциденти та відсутність чітких критеріїв оцінки ефективності системи [6].

Постанова КМУ "Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі" від 4 квітня 2023 року № 299 доповнює попередню, окреслюючи більш детальні алгоритми реагування на кіберінциденти. Ключовими положеннями є: визначення послідовності етапів реагування на кіберінциденти (виявлення, аналіз, стримування, усунення, відновлення); запровадження системи класифікації кіберінцидентів за рівнями критичності; передбачається розробка детальних методичних рекомендацій для суб'єктів кібербезпеки. Однак залишається відкритим питання ефективності реалізації методичних рекомендацій, а також недостатньо уваги приділено питанням відповідальності за невиконання вимог. Отже, вказані документи є важливим кроком у розвитку системи кібербезпеки в Україні. Вони створюють нормативно-правову базу для забезпечення ефективного реагування на кіберінциденти у інформаційних системах [7].

У цьому зв'язку видається важливим гармонізація національного законодавства з міжнародними практиками, наприклад, на основі міжнародних стандартів ISO/IEC 27035, які розроблені спільно Міжнародною організацією зі стандартизації (ISO) і Міжнародною електротехнічною комісією (IEC) та надають детальні рекомендації щодо управління інцидентами інформаційної та кібернетичної безпеки. Ці стандарти є своєрідним посібником для організацій, що допомагає їм ефективно виявляти, аналізувати, реагувати та відновлюватися після кібератак та інших інцидентів, пов'язаних з безпекою інформаційних систем. ISO/IEC 27035 є міжнародно визнаними стандартами, що свідчить про їхню релевантність та актуальність [8].

Усуваючи ці прогалини, Україна зможе створити більш ефективну та надійну систему кібербезпеки, яка відповідатиме сучасним викликам та загрозам. Чітка деталізація положень у законодавстві дозволить органам державної влади та приватним компаніям краще розуміти свої обов'язки та відповідальність, а також забезпечить більш скоординовану та ефективну боротьбу з кіберзагрозами.

Наступним безпековим викликом цифрової взаємодії органів публічної влади є відсутність конкретних стандартів і вимог до кібербезпеки для різних сфер публічного управління, зокрема критичної інфраструктури. Цифрова трансформація органів публічної влади ставить перед суспільством нові виклики у сфері кібербезпеки, особливо коли мова йде про критичну інфраструктуру. Критична інфраструктура охоплює життєво важливі об'єкти, що забезпечують функціонування суспільства, такі як енергетика, транспорт, зв'язок, охорона здоров'я тощо.

Правові рамки та ініціативи для захисту критичної інфраструктури впроваджено низкою розвинутих країн. У Європейському Союзі основними інструментами для підвищення безпеки та стійкості критичної інфраструктури є Директива NIS-2 і Директива CER.

Важливість NIS 2.0 полягає в її комплексному підході, яка охоплює не лише технічні аспекти, але й організаційні та нормативні аспекти мережевої та інформаційної безпеки. Запроваджуючи суворіші правила та чітко визначені стандарти безпеки, NIS 2.0 встановлює нові стандарти захисту критичної інфраструктури та цифрових послуг у Європі. Директива NIS-2 спрямована на забезпечення високого рівня безпеки мережевих та інформаційних систем в ЄС. Вона розширює перелік секторів, які вважаються критичними, і посилює транскордонне співробітництво між країнами-членами [9].

Директива CER націлена на підвищення стійкості критичної інфраструктури до різних загроз. Вона вимагає від держав-членів запровадження заходів для покращення фізичної та операційної безпеки критичних об'єктів. Це включає визначення критичної інфраструктури в різних секторах, регулярні оцінки ризиків та загроз, а також розробку та впровадження стратегій управління надзвичайними ситуаціями та кризами [10].

Особливе значення критичної інфраструктури зумовлено кількома факторами: системною важливістю, взаємозалежністю та привабливістю для кіберзлочинців. Ці об'єкти забезпечують життєво важливі послуги, від яких залежить стабільність та функціонування суспільства. Відомо, що порушення роботи одного об'єкта критичної інфраструктури призводить до каскадних ефектів, паралізуючи цілі сектори економіки. Важливість цих об'єктів робить їх привабливою мішенню для кібератак, а відсутність чітко визначених стандартів кібербезпеки створює серйозні ризики для виникнення вразливостей, які можуть бути використані

кіберзлочинцями. Кібератаки на критичну інфраструктуру обумовлюють економічні втрати через перебої у роботі підприємств, втрату даних та репутаційні збитки та використовуються як інструмент гібридної війни, що створює геополітичні ризики.

Щоб розв'язати ці проблеми, необхідно розробити національні стандарти кібербезпеки для критичної інфраструктури, враховуючи специфіку різних сфер публічного управління. Всі об'єкти критичної інфраструктури повинні пройти сертифікацію на відповідність вимогам стандартів кібербезпеки.

Недостатня координація між державними органами є ще одним безпековим викликом та ключовою проблемою у цьому контексті. Відсутність ефективних механізмів координації та співпраці між різними державними органами, які відповідають за кібербезпеку, ускладнює обмін інформацією та спільне реагування на кіберінциденти. Така розрізненість зусиль призводить до того, що навіть у разі наявності окремих ініціатив з посилення кібербезпеки, загальний рівень захисту залишається недостатнім через відсутність скоординованого підходу та об'єднаних ресурсів.

В Україні дійсно створено декілька структур, які відповідають за забезпечення кібербезпеки. Однак, наскільки ефективною є їхня робота та чи можна говорити про створення єдиного потужного центру кібербезпеки, є предметом дискусій.

Однією з таких структур є Державний центр кіберзахисту Державного агентства спеціального зв'язку та захисту інформації. Цей центр виконує важливі функції з підвищення рівня кіберзахисту державних інформаційних ресурсів [11]. Однак, незважаючи на наявність цього центру, загальна картина кібербезпеки в Україні залишається складною.

Національний координаційний центр кібербезпеки є робочим органом Ради національної безпеки і оборони України, відповідальним за координацію зусиль різних органів державної влади у сфері кібербезпеки [12]. Проте ефективність його роботи часто піддається критиці через недостатнє фінансування та обмежені повноваження.

Державне підприємство "Галузевий центр кібербезпеки" сфокусоване на питаннях кібербезпеки в інфраструктурних секторах [13].

Існує декілька ключових проблем, які заважають ефективній роботі в галузі кібербезпеки. По-перше, відповідальність за кібербезпеку розподілена між різними органами публічної влади, що ускладнює координацію їхніх дій. По-друге, бюджетні асигнування на кібербезпеку є недостатніми для ефективного вирішення проблем. Крім того, існує дефіцит висококваліфікованих фахівців у сфері кібербезпеки, що ще більше ускладнює ситуацію. Також часто відсутня єдина стратегія, яка б чітко визначала національні пріоритети та цілі у сфері кібербезпеки.

Незважаючи на існування окремих структур, які займаються питаннями кібербезпеки в Україні, їхня ефективність потребує значного покращення. Для створення дієвої системи кібербезпеки необхідно вирішити проблеми координації, фінансування та кадрового забезпечення. Це дозволить забезпечити більш надійний захист критичної інфраструктури та підвищити рівень кібербезпеки в країні.

Для вирішення цих проблем необхідно вжити низку заходів. По-перше, створити єдину систему координації кібербезпеки, який би координував усі зусилля на усіх рівнях управління та мав широкі повноваження. По-друге, необхідно значно збільшити фінансування заходів з кібербезпеки. Також слід розробити довгострокову стратегію кібербезпеки, яка визначить пріоритети та цілі на найближчі роки. Підвищення рівня обізнаності населення через масштабні інформаційні кампанії також є важливим кроком. Крім того, необхідно активно залучати потенціал приватного сектору до розробки та впровадження заходів з кібербезпеки. Враховуючи існування Державного центру кіберзахисту Держспецзв'язку, його необхідно інтегрувати в єдину систему координації кібербезпеки та наділити його більш широкими повноваженнями, який би об'єднав зусилля всіх існуючих структур, що є ключовим кроком для підвищення рівня кібербезпеки в Україні.

Однак, проблема координації є лише одним з викликів, що стосується більш широкого питання — обмеженого фінансування та ресурсів. Недостатнє фінансування та технічне забезпечення державних органів, що відповідають за кібербезпеку, значно обмежують їхні можливості ефективно реагувати на кіберзагрози. Без належних фінансових ресурсів складно впроваджувати передові технології та розробляти ефективні стратегії захисту. Цей чинник значно обмежує можливості ефективно протистояти кіберзагрозам, які постійно зростають у масштабах та складності.

Сучасні технології, які використовуються кіберзлочинцями, постійно вдосконалюються, і для ефективного протистояння їм необхідні аналогічні інструменти та програмне забезпечення. Швидкість реакції на кіберінциденти є критично важливою, відтак без належного фінансування впровадження сучасних систем моніторингу та аналізу загроз своєчасне виявлення та нейтралізація атак видається малоймовірним.

Використання штучного інтелекту (AI) та машинного навчання (ML) в кібербезпеці є значним прогресом у цій галузі. Ці технології дозволяють обробляти величезні обсяги даних з безпрецедентною швидкістю, що робить їх безцінними інструментами в боротьбі з кіберзлочинністю. Однією з ключових переваг AI та ML у кібербезпеці є їхня здатність навчатися та адаптуватися з часом. У міру того, як розвиваються кіберзагрози, змінюються і алгоритми, які використовуються для їх виявлення та протидії. Ще однією суттєвою перевагою є автоматизація рутинних завдань, що вивільняє людські ресурси для більш складних та стратегічних дій. AI та ML можуть автоматизувати виявлення аномалій і потенційних загроз, дозволяючи фахівцям з кібербезпеки зосередитися на прийнятті рішень і стратегіях реагування на вищому рівні. Оскільки ці технології продовжують розвиватися, вони відіграватимуть дедалі важливішу роль у захисті цифрових активів та інформаційних систем органів публічної влади, що й потребує відповідного фінансового забезпечення [14]. Згідно зі звітом Cybersecurity Ventures, глобальні економічні збитки від кібератак досягнуть 10,5 трильйонів доларів США до 2025 року [15].

Недостатнє фінансування та технічне забезпечення державних органів, відповідальних за кібербезпеку, призводить не лише до обмежених можливостей у протидії кіберзагрозам, але й до серйозних кадрових про-

блем. Зазначене дозволяє виокремити ще один безпековий виклик, що проявляється у нестачі кваліфікованих фахівців у сфері кібербезпеки та обмежені можливості щодо підвищення кваліфікації тих, хто отримав освіту декілька років назад. Відсутність достатньої кількості спеціалістів значно ускладнює боротьбу з кіберзагрозами. Ця проблема тісно пов'язана з недостатнім фінансуванням та технічним забезпеченням, оскільки саме відсутність інвестицій у розвиток людського капіталу стримує розвиток галузі.

Відомо, що сучасні кібератаки стають все більш складними та витонченими, що вимагає від фахівців високої кваліфікації та постійного оновлення знань. Технології в сфері кібербезпеки розвиваються дуже швидко, і фахівці повинні постійно вчитися новому. Крім того, висококваліфіковані фахівці з кібербезпеки користуються великим попитом на світовому ринку праці, що ускладнює їх залучення та утримання в Україні.

Наслідки дефіциту фахівців проявляються у затримках у виявленні та усуненні вразливостей, неефективному реагуванні на кіберінциденти та збільшенні кількості кібератак. Недостатня кількість кваліфікованих фахівців ускладнює швидке та ефективне реагування на кіберінциденти, створюючи сприятливі умови для кіберзлочинців. Багато випадків витоку даних пов'язані з людським фактором, тобто з помилками співробітників, які не мають достатньої кваліфікації. Відсутність достатньої кількості фахівців з цифрової криміналістики ускладнює проведення розслідувань кіберзлочинів. Органи публічної влади відчувають гостру нестачу фахівців з кібербезпеки, що негативно впливає на їхню здатність захищати власні інформаційні системи.

Для вирішення цієї проблеми необхідно розвивати спеціалізовані освітні програми в галузі кібербезпеки на всіх рівнях освіти, створювати систему постійного підвищення кваліфікації фахівців, залучати приватні компанії до підготовки кадрів та створювати спільні навчальні програми. Заохочення молоді до обрання професії в галузі кібербезпеки та розширення міжнародного співробітництва для обміну досвідом і залучення іноземних експертів також є важливими кроками.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Отже, для ефективного забезпечення кібербезпеки в Україні необхідно здійснити комплексні заходи на державному рівні. В першу чергу, необхідно розробити єдину державну стратегію кібербезпеки. Ця стратегія повинна визначити пріоритети, цілі та заходи, необхідні для захисту інформаційних систем країни. Її реалізація дозволить забезпечити узгодженість дій різних відомств і організацій у сфері кібербезпеки.

Крім того, важливим кроком є удосконалення законодавчої бази. Необхідно деталізувати законодавство у сфері кібербезпеки, встановити чіткі вимоги до захисту інформації та відповідальність за її порушення. Це створить правові основи для ефективного реагування на кіберзагрози та забезпечить відповідальність за недотримання вимог безпеки.

Збільшення фінансування також є критично важливим. Необхідно значно збільшити бюджетні видатки на кібербезпеку для забезпечення необхідних ресурсів для захисту інформаційних систем. Це включає закупівлю сучасного обладнання, програмного забезпечення, а також фінансування наукових досліджень та розробок у цій галузі.

Розвиток системи підготовки кадрів є ще одним ключовим елементом. Слід розвивати спеціалізовані освітні програми в галузі кібербезпеки, створювати систему постійного підвищення кваліфікації фахівців та залучати приватний сектор до підготовки кадрів. Це дозволить забезпечити високий рівень професійної підготовки фахівців та відповідати на сучасні виклики кібербезпеки.

Також важливим аспектом є посилення ролі громадянського суспільства. Залучення громадянського суспільства до обговорення питань кібербезпеки та підвищення рівня кібергігієни населення сприятиме більшій обізнаності та відповідальності громадян у сфері кібербезпеки. Це дозволить створити більш стійку та захищену інформаційну інфраструктуру на всіх рівнях та ефективно протистояти сучасним кіберзагрозам.

Таким чином, цифрова взаємодія органів публічної влади в Україні є невідворотнім процесом, який відкриває нові можливості для підвищення ефективності та прозорості надання державних послуг. Водночас, цей процес супроводжується значними безпековими викликами, пов'язаними з недостатньою законодавчою базою (відсутністю чітких норм та стандартів у сфері кібербезпеки, що ускладнює ефективне впровадження заходів захисту); відсутністю єдиної стратегії кібербезпеки (роздробленістю відповідальності за кібербезпеку між різними органами публічної влади, що перешкоджає координації зусиль та ефективному реагуванню на кіберзагрози); обмеженими фінансовими ресурсами (недостатністю фінансування, слабким рівнем сучасного обладнання, програмного забезпечення, обмеженими можливостями для підвищення кваліфікації фахівців); дефіцитом кваліфікованих кадрів, що призводить до неналежного рівня захисту інформаційних систем.

Література:

1. European Center for Digital Competitiveness — Digitalreport 2022. URL: https://digital-competitiveness.eu/wp-content/uploads/Digitalreport-2022.pdf

2. EIB report on digitalization in Europe 2021/2022: The pandemic has anchored digital change in European society. URL: https://www.eib.org/en/publications/digitalisation-in-europe-2021-2022

3. K. Karhu, R. Gustafsson, B. Eaton etc. Four Tactics for Implementing a Balanced Digital Platform Strategy. MIS quarterly executive. 2020, Vol. 19 (2), pp. 105—120.

4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

5. Про внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації: Закон України від 4 червня 2020 року № 681-IX. URL: https://zakon.rada.gov.ua/laws/show/681-20#Text

6. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова КМУ від 23 грудня 2020 року № 1295. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text

7. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова КМУ від 4 квітня 2023 року № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text

8. ISO/IEC 27035-1:2023 Information technology — Information security incident management — Part 1: Principles and process. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-2:v1:en

9. NIS 2.0 Directive — Comprehensive guide on NIS 2. URL: https://safereach.com/en/blog/nis-2-directive/

10. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

11. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua

12. Національний координаційний центр кібербезпеки. URL: https://report@ncscc.gov.ua/

13. Галузевий центр кібербезпеки сприятиме забезпеченню надійного захисту підприємств енергетичного сектору. URL: https://www.kmu.gov.ua/news/galuzevij-centr-kiberbezpeki-spriyatime-zabezpechennyu-nadijnogo-zahistu-pidpriyemstv-energetichnogo-sektoru

14. T. Abrahams, S. Ewuga. A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, Volume 5, Issue 1, January 2024. URL: https://www.researchgate.net/publication/377346019_A_review_of_cybersecurity_strategies_in_modern_organizations_examining_the_evolution_and_effectiveness_of_cybersecurity_measures_for_data_protection

15. World Economic Forum. Why we need global rules to crack down on cybercrime. Jan 2, 2023. URL: https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/

References:

1. European Center for Digital Competitiveness (2022), "Digitalreport", available at: https://digital-competitiveness.eu/wp-content/uploads/Digitalreport-2022.pdf (Accessed 25 July 2024).

2. EIB (2022), "EIB report on digitalization in Europe 2021/2022: The pandemic has anchored digital change in European society", available at: https://www.eib.org/en/publications/digitalisation-in-europe-2021-2022 (Accessed 25 July 2024).

3. Karhu, K. Gustafsson, R. and Eaton, B. (2020), "Four Tactics for Implementing a Balanced Digital Platform Strategy", MIS quarterly executive, vol. 19 (2), pp.105-120

4. Verkhovna Rada of Ukraine (1994), The Law of Ukraine "On Protection of Information in Automated Systems", available at: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (Accessed 25 June 2024).

5. Verkhovna Rada of Ukraine (2020), The Law of Ukraine "On making amendments to the Law of Ukraine "On Information Protection in Information and Telecommunication Systems" regarding confirmation of information system compliance with information protection requirements", available at: https://zakon.rada.gov.ua/laws/show/681-20#Text (Accessed 25 June 2024).

6. Cabinet of Ministers of Ukraine (2020), Resolution "Some issues of ensuring the functioning of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks", available at: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text (Accessed 25 July 2024).

7. Cabinet of Ministers of Ukraine (2023), Resolution "Some issues of response by cyber security entities to various types of events in cyberspace", available at: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text (Accessed 25 July 2024).

8. ISO (2023), "ISO/IEC 27035-1:2023 Information technology — Information security incident management — Part 1: Principles and process", available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-2:v1:en (Accessed 25 July 2024).

9. safeREACH (2023), "NIS 2.0 Directive — Comprehensive guide on NIS 2", available at: https://safereach.com/en/blog/nis-2-directive/ (Accessed 25 July 2024).

10. Official Journal of the European Union (2022), "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC", available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj (Accessed 25 July 2024).

11. State Service for Special Communications and Information Protection of Ukraine (2024), available at: https://cip.gov.ua/ua (Accessed 25 July 2024).

12. National Cyber Security Coordination Center (2024), available at: https://ncscc.gov.ua/ (Accessed 25 July 2024).

13. Government portal (2019), "The cyber security industry center will contribute to ensuring reliable protection of energy sector enterprises", available at: https://www.kmu.gov.ua/news/galuzevij-centr-kiberbezpeki-spriyatime-zabezpechennyu-nadijnogo-zahistu-pidpriyemstv-energetichnogo-sektoru (Accessed 25 July 2024).

14. Abrahams, T. and Ewuga, S. (2024), "A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection", Computer Science & IT Research Journal, vol. 5, iss. 1, available at: https://www.researchgate.net/publication/377346019_A_review_of_cybersecurity_strategies_in_modern_organizations_examining_the_evolution_and_effectiveness_of_cybersecurity_measures_for_data_protection (Accessed 25 July 2024).

15. World Economic Forum (2023), "Why we need global rules to crack down on cybercrime", available at: https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/ (Accessed 25 July 2024).

Стаття надійшла до редакції 04.08.2024 р.