УДК 004.056:35
DOI https://doi.org/10.32782/TNU-2663-6468/2026.5/28

Прохорський С. І.
https://orcid.org/0000-0002-6369-2601
Акціонерне товариство Українська залізниця

Шорнікова С. В.
https://orcid.org/0000-0002-5430-6502
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби Безпеки України

Євстратенко С. М.
https://orcid.org/0009-0009-5148-1813

ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ УСТАНОВ ДЕРЖАВНОГО СЕКТОРУ

У статті досліджено особливості забезпечення кіберстійкості установ державного сектору в умовах зростання кількості та складності кіберзагроз, цифровізації управлінських процесів і підвищення залежності державних інституцій від інформаційно-комунікаційних систем. Обґрунтовано, що кіберстійкість є однією з ключових передумов стабільного функціонування органів державної влади, збереження цілісності, конфіденційності та доступності інформаційних ресурсів, а також безперервності надання публічних послуг.

Увагу зосереджено на сутності поняття кіберстійкості як здатності установи запобігати кіберінцидентам, виявляти їх, ефективно реагувати на них, мінімізувати наслідки та швидко відновлювати працездатність критично важливих систем і сервісів. Визначено, що для установ державного сектору забезпечення кіберстійкості має базуватися на комплексному підході, який поєднує організаційні, нормативно-правові, кадрові та технічні заходи.

У статті проаналізовано основні чинники, що впливають на рівень кіберстійкості державних установ, зокрема стан захищеності інформаційної інфраструктури, рівень зрілості процесів управління інформаційною безпекою, наявність механізмів моніторингу та реагування на інциденти, підготовленість персоналу до дій в умовах кіберзагроз, а також ефективність міжвідомчої координації. Наголошено, що одними з найбільш поширених загроз для державного сектору є фішинг, шкідливе програмне забезпечення, атаки типу ransomware, компрометація облікових записів, DDoS-атаки та спроби несанкціонованого доступу до державних інформаційних ресурсів.

Окреслено практичні напрями підвищення кіберстійкості установ державного сектору, серед яких впровадження політик інформаційної безпеки, багаторівневого захисту інформаційних систем, систем резервного копіювання та відновлення даних, постійного моніторингу подій безпеки, сучасних засобів виявлення і реагування на інциденти, а також проведення регулярного навчання персоналу. Підкреслено значення ризик-орієнтованого підходу до управління кібербезпекою та необхідність інтеграції заходів кіберзахисту в загальну систему державного управління.

Зроблено висновок, що забезпечення кіберстійкості установ державного сектору є безперервним процесом, який потребує системного вдосконалення механізмів кіберзахисту, адаптації до нових типів загроз і розвитку інституційної спроможності держави у сфері кібербезпеки. Реалізація комплексних заходів у цій сфері сприятиме підвищенню надійності функціонування державних інформаційних систем, зміцненню довіри до публічного управління та посиленню національної безпеки.

Ключові слова: *кіберстійкість, кібербезпека, державний сектор, державні установи, кіберзагрози, інформаційна безпека, захист інформаційних систем, реагування на інциденти, управління ризиками, публічне управління.*

© Косаревич Н. Б., Шорнікова С. В., Мануляк Р. Т., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

Постановка проблеми. Сучасний етап розвитку державного сектору характеризується активною цифровізацією управлінських процесів, упровадженням електронного урядування, розширенням використання інформаційно-комунікаційних систем та зростанням обсягів обробки даних. За таких умов установи державного сектору стають об'єктами підвищеної уваги з боку кіберзлочинців, оскільки саме в їхніх інформаційних системах зосереджено значні масиви службової, персональної та стратегічно важливої інформації. Це зумовлює необхідність посилення захисту державних інформаційних ресурсів і забезпечення безперервності функціонування публічних сервісів.

Актуальність проблеми посилюється постійним зростанням кількості кіберінцидентів, ускладненням методів кібератак, поширенням шкідливого програмного забезпечення, фішингових кампаній, атак на облікові записи, мережеву інфраструктуру та критично важливі інформаційні системи. Особливу небезпеку для установ державного сектору становлять атаки, спрямовані не лише на викрадення чи знищення даних, а й на порушення стабільності управлінських процесів, блокування роботи державних сервісів, підрив довіри громадян до органів влади та послаблення інституційної спроможності держави.

У зв'язку з цим традиційного підходу до кібербезпеки, що зосереджується переважно на запобіганні загрозам, уже недостатньо. Натомість дедалі більшого значення набуває концепція кіберстійкості, яка передбачає здатність установи не лише протидіяти кіберзагрозам, а й своєчасно їх виявляти, локалізувати наслідки, підтримувати критичні функції та швидко відновлювати працездатність після кіберінцидентів. Саме такий підхід є особливо важливим для державного сектору, де навіть короткочасне порушення функціонування інформаційних систем може мати значні соціальні, економічні та безпекові наслідки.

Попри зростання уваги до питань кібербезпеки, у практиці функціонування установ державного сектору все ще зберігаються проблеми недостатньої зрілості систем управління інформаційною безпекою, обмеженості ресурсного забезпечення, фрагментарності організаційно-технічних заходів, недостатнього рівня підготовки персоналу та потреби в удосконаленні координації між суб'єктами кіберзахисту. Це актуалізує необхідність наукового осмислення підходів до забезпечення кіберстійкості установ державного сектору та визначення ефективних заходів її підвищення.

Отже, проблема забезпечення кіберстійкості установ державного сектору полягає в необхідності формування комплексної системи організаційних, технічних, кадрових і управлінських заходів, здатної забезпечити належний рівень захисту інформаційних ресурсів, стійкість до сучасних кіберзагроз і безперервність виконання державними установами своїх функцій.

Аналіз останніх досліджень і публікацій. Проблематика забезпечення кіберстійкості установ державного сектору посідає важливе місце в сучасних наукових дослідженнях, оскільки поєднує питання кібербезпеки, захисту інформаційних ресурсів, управління ризиками, цифрової трансформації та безперервності функціонування державних інституцій. У працях вітчизняних і зарубіжних науковців кіберстійкість розглядається як комплексна характеристика здатності інформаційних систем та організацій протидіяти кіберзагрозам, адаптуватися до інцидентів і забезпечувати відновлення після порушень [1; 2].

Суттєвий внесок у формування теоретичних підходів до розуміння кіберстійкості зроблено в межах міжнародних стандартів і рекомендацій, зокрема документів NIST, у яких обґрунтовано ризик-орієнтований підхід до управління кібербезпекою, визначено основні функції ідентифікації, захисту, виявлення, реагування та відновлення [3]. У цьому контексті кіберстійкість державних установ розглядається не лише як технічний стан захищеності, а як результат інтегрованого управління ризиками, процесами реагування на інциденти та забезпечення безперервності діяльності [3; 4].

Значну увагу в сучасних дослідженнях приділено питанням кібербезпеки державного сектору в умовах цифровізації. Науковці підкреслюють, що розширення електронного урядування, використання хмарних сервісів, міжвідомчих інформаційних систем та електронного документообігу одночасно підвищує ефективність публічного управління і збільшує поверхню атаки для потенційних зловмисників [5; 6]. У зв'язку з цим обґрунтовується потреба в посиленні організаційно-правових і технічних заходів кіберзахисту саме в установах державного сектору [6; 7].

У працях, присвячених захисту державних інформаційних ресурсів, акцентується увага на важливості створення системи постійного моніторингу подій безпеки, упровадження засобів виявлення та реагування на інциденти, багаторівневого захисту мережевої інфраструктури, резервного копіювання та регулярного аудиту вразливостей [4; 8]. Дослідники також наголошують, що тех-

нічні інструменти не забезпечують належного рівня кіберстійкості без належної підготовки персоналу, формування культури кібербезпеки та чіткого розподілу відповідальності в організаційній структурі установи [2; 7; 9].

Окремий напрям наукових публікацій стосується нормативно-правового забезпечення кібербезпеки в Україні. У цій площині важливе значення мають Закон України «Про основні засади забезпечення кібербезпеки України», Стратегія кібербезпеки України, а також підзаконні акти, що визначають організаційні та інституційні механізми захисту державних інформаційних ресурсів [10; 11]. Зазначені документи формують базові умови для розвитку системи кіберзахисту, однак у наукових працях підкреслюється необхідність подальшого вдосконалення механізмів практичної реалізації політики кіберстійкості в установах державного сектору [6; 11].

Таким чином, аналіз останніх досліджень і публікацій свідчить, що проблема забезпечення кіберстійкості установ державного сектору є комплексною та міждисциплінарною. Незважаючи на значну кількість наукових праць і нормативних документів, потребують подальшого дослідження питання розроблення ефективних моделей підвищення кіберстійкості державних установ, адаптованих до сучасних загроз, обмежених ресурсів і потреби забезпечення безперервності надання публічних послуг.

Постановка завдання. Метою статті є систематизація сучасних підходів до забезпечення кіберстійкості установ державного сектору та визначення ефективних організаційно-технічних механізмів протидії кіберзагрозам у процесі функціонування державних інформаційних систем.

Виклад основного матеріалу. У сучасних умовах цифрової трансформації державного управління питання забезпечення кіберстійкості установ державного сектору набуває особливої актуальності [1; 3]. Широке впровадження електронного документообігу, державних реєстрів, інформаційно-комунікаційних систем, хмарних сервісів і платформ електронної взаємодії створює нові можливості для підвищення ефективності діяльності органів влади, однак одночасно збільшує кількість потенційних вразливостей і розширює поверхню кібератак [5; 6]. За таких умов кіберстійкість слід розглядати як невід'ємну складову належного функціонування державних установ, що забезпечує не лише захист інформаційних ресурсів, а й спроможність організації підтримувати виконання своїх ключових функцій у разі виникнення кіберінцидентів [3; 8].

Кіберстійкість установ державного сектору доцільно трактувати як здатність організації прогнозувати, запобігати, виявляти, локалізувати та долати наслідки кіберзагроз, зберігаючи при цьому прийнятний рівень функціонування інформаційних систем і публічних сервісів [3; 10]. На відміну від традиційного підходу до кібербезпеки, який переважно орієнтований на запобігання несанкціонованому доступу, кіберстійкість акцентує увагу на безперервності діяльності, адаптивності та здатності до швидкого відновлення після інциденту [4; 8]. Саме тому в державному секторі вона має розглядатися як стратегічний елемент системи управління ризиками та державної безпеки [6; 11].

Однією з основних передумов забезпечення кіберстійкості є формування комплексної системи управління кібербезпекою в установі [2; 7]. Така система повинна охоплювати організаційний, нормативний, технічний і кадровий рівні. На організаційному рівні важливим є визначення відповідальних осіб за кібербезпеку, розподіл повноважень, розроблення внутрішніх політик безпеки, регламентів реагування на інциденти та процедур взаємодії між структурними підрозділами [7; 9]. На нормативному рівні необхідним є приведення внутрішніх документів установи у відповідність до вимог національного законодавства та галузевих стандартів у сфері кіберзахисту [10; 11].

Технічна складова кіберстійкості передбачає впровадження багаторівневого захисту інформаційної інфраструктури [3; 7; 8]. Йдеться про використання міжмережевих екранів, систем виявлення та запобігання вторгненням, засобів антивірусного захисту, технологій EDR/XDR, багатофакторної автентифікації, сегментації мережі, криптографічного захисту даних, систем резервного копіювання та відновлення [4; 8]. Ефективність технічних рішень значною мірою залежить від належної конфігурації, регулярного оновлення, моніторингу подій безпеки та своєчасного усунення вразливостей [3; 4].

Важливим напрямом зміцнення кіберстійкості є впровадження ризик-орієнтованого підходу [3; 8]. Для установ державного сектору це означає систематичну ідентифікацію критичних інформаційних ресурсів, оцінювання потенційних загроз, визначення рівня вразливості активів і прогнозування можливих наслідків реалізації кіберризиків [3]. На основі такої оцінки можуть визначатися пріоритети фінансування заходів безпеки, розподіл ресурсів, планування аудиту та тестування систем

захисту [6; 8]. Ризик-орієнтований підхід дозволяє перейти від реактивної моделі захисту до проактивного управління кіберзагрозами [1; 3].

Суттєву роль у забезпеченні кіберстійкості відіграє безперервний моніторинг подій інформаційної безпеки та готовність до реагування на інциденти [4; 8]. Установи державного сектору повинні мати процедури виявлення підозрілої активності, оброблення інцидентів, локалізації загроз, фіксації цифрових слідів і відновлення працездатності систем [4]. Доцільним є використання централізованих платформ моніторингу, зокрема SIEM, XDR та UEBA-рішень, які забезпечують кореляцію подій із різних джерел, виявлення аномальної поведінки користувачів і пристроїв, а також оперативне інформування відповідальних підрозділів [8; 9]. За відсутності належного моніторингу навіть технічно захищені системи залишаються вразливими до прихованих або тривалих атак [3; 4].

Окрему увагу слід приділити підготовці персоналу, оскільки людський фактор залишається одним із найслабших елементів системи кіберзахисту [2; 9]. Працівники державних установ мають володіти базовими знаннями з кібергігієни, розпізнавання фішингових повідомлень, безпечної роботи з документами, паролями, зовнішніми носіями та хмарними сервісами [6; 9]. Для цього необхідно проводити регулярне навчання, інструктажі, тестування обізнаності та моделювання інцидентів [7; 9]. Підвищення рівня кіберкультури персоналу сприяє зменшенню кількості помилок, що можуть призвести до компрометації державних інформаційних систем [2; 6].

Не менш важливим є забезпечення безперервності діяльності установ державного сектору в умовах кіберінцидентів [3; 4]. Для цього повинні розроблятися та регулярно оновлюватися плани реагування на інциденти, плани аварійного відновлення, резервування критичних даних і сервісів [4; 8]. Кіберстійкість не обмежується запобіганням атакам; вона передбачає наявність спроможності організації функціонувати навіть за умов часткової втрати інформаційних ресурсів або тимчасового порушення роботи окремих систем [3; 8]. Саме така спроможність є ключовою для державного сектору, де збої в роботі інформаційної інфраструктури можуть мати широкий суспільний резонанс [6; 11].

Особливого значення набуває міжвідомча координація у сфері кіберзахисту [10; 11]. Кіберзагрози для державного сектору часто мають комплексний і скоординований характер, тому ефективне реагування потребує обміну інформацією між державними установами, центрами реагування на інциденти, суб'єктами національної системи кібербезпеки та правоохоронними органами [6; 10]. Така взаємодія сприяє оперативному виявленню нових схем атак, поширенню індикаторів компрометації та виробленню спільних механізмів протидії [10; 11].

Отже, забезпечення кіберстійкості установ державного сектору є багаторівневим процесом, що передбачає інтеграцію управлінських рішень, нормативно-правового регулювання, технічного захисту, постійного моніторингу, навчання персоналу та планування відновлення діяльності після інцидентів [1; 3; 11]. Лише комплексний підхід до реалізації зазначених заходів дає змогу сформувати стійку систему кіберзахисту, здатну ефективно протидіяти сучасним загрозам і гарантувати безперервність функціонування державних установ [3; 8].

Висновки. У результаті проведеного дослідження встановлено, що забезпечення кіберстійкості установ державного сектору є однією з ключових умов стабільного функціонування державних інституцій в умовах цифрової трансформації та постійного зростання кіберзагроз [1; 6]. Доведено, що кіберстійкість доцільно розглядати не лише як технічну захищеність інформаційних систем, а як комплексну здатність установи запобігати кіберінцидентам, своєчасно їх виявляти, локалізувати наслідки, підтримувати критичні процеси та швидко відновлювати свою діяльність [3; 4; 8].

Обґрунтовано, що ефективне підвищення рівня кіберстійкості потребує комплексного поєднання організаційних, правових, кадрових і технічних заходів [2; 7; 10]. До найбільш важливих із них належать формування політик інформаційної безпеки, впровадження ризик-орієнтованого підходу, використання сучасних засобів моніторингу та реагування на інциденти, резервного копіювання й відновлення даних, а також систематичне підвищення рівня обізнаності персоналу з питань кібергігієни [4; 8; 9].

Визначено, що особливістю державного сектору є висока критичність інформаційних ресурсів, значна суспільна важливість безперервності надання публічних послуг та необхідність координації між різними суб'єктами кіберзахисту [6; 10; 11]. У зв'язку з цим забезпечення кіберстійкості установ державного сектору має здійснюватися на основі системного підходу, що враховує як внутрішні організаційні можливості установи, так і зовнішні загрози, нормативні вимоги та інституційну взаємодію.

Отже, підвищення кіберстійкості установ державного сектору слід розглядати як безперервний процес удосконалення управлінських механізмів, технологічних рішень і кадрового потенціалу, спрямований на зміцнення захищеності державних інформаційних ресурсів, забезпечення стійкості до кіберзагроз і підвищення довіри до системи публічного управління.

Список літератури:

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Київ : ДУТ, 2015. 288 с.

2. Ліпкан В. А. Інформаційна безпека України : монографія. Київ : КНТ, 2006. 576 с.

3. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD : NIST, 2018. 55 p.

4. National Institute of Standards and Technology. Computer Security Incident Handling Guide. Gaithersburg, MD : NIST, 2012. 79 p.

5. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика : монографія. Київ : Вид. дім «АртЕк», 2014. 434 с.

Дубов Д. В. Кібербезпекова політика України у сфері державного управління. Київ : НІСД, 2021. 196 с.

6. Корченко О. Г., Гордійчук А. А., Архипов О. Є. Системи захисту інформації : навч. посіб. Київ : Лазурит-Поліграф, 2015. 600 с.

7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : ISO, 2022.

8. Peltier T. R. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Boca Raton : Auerbach Publications, 2016. 408 p.

9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

10. Стратегія кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

Prokhorskyy S. I., Shornikova S. V., Yevstratenko S. M. ENSURING CYBER RESILIENCE OF PUBLIC SECTOR INSTITUTIONS

The article examines the theoretical and practical aspects of ensuring the cyber resilience of public sector institutions in the context of the growing number and complexity of cyber threats, digital transformation of public administration, and increasing dependence of state institutions on information and communication systems. It is substantiated that cyber resilience is one of the key prerequisites for the stable functioning of public authorities, preservation of the integrity, confidentiality, and availability of information resources, as well as continuity of public service delivery.

The study focuses on the essence of cyber resilience as the ability of an institution to prevent cyber incidents, detect them in a timely manner, respond effectively, minimize consequences, and quickly restore the operation of critical systems and services. It is determined that for public sector institutions, cyber resilience should be based on an integrated approach combining organizational, regulatory, personnel, and technical measures.

The article analyzes the main factors influencing the level of cyber resilience of public institutions, including the state of protection of information infrastructure, maturity of information security management processes, availability of monitoring and incident response mechanisms, staff preparedness to act under cyber threats, and the effectiveness of interagency coordination. It is emphasized that among the most common threats to the public sector are phishing, malware, ransomware attacks, account compromise, distributed denial-of-service attacks, and attempts of unauthorized access to public information resources.

Practical directions for increasing the cyber resilience of public sector institutions are outlined, including the implementation of information security policies, layered protection of information systems, backup and data recovery systems, continuous monitoring of security events, modern incident detection and response tools, and regular staff training. The importance of a risk-oriented approach to cybersecurity management and the need to integrate cyber protection measures into the overall public administration system are highlighted.

It is concluded that ensuring the cyber resilience of public sector institutions is a continuous process that requires systematic improvement of cyber defense mechanisms, adaptation to new types of threats,

and strengthening the institutional capacity of the state in the field of cybersecurity. The implementation of comprehensive measures in this area will help increase the reliability of public information systems, strengthen trust in public administration, and enhance national security.

Keywords: *cyber resilience, cybersecurity, public sector, public institutions, cyber threats, information security, protection of information systems, incident response, risk management, public administration.*

Дата першого надходження статті до видання: 11.09.2026
Дата прийняття статті до друку після рецензування: 28.09.2026
Дата публікації (оприлюднення) статті: 16.11.2026