УДК 351:4
DOI https://doi.org/10.32782/pdu.2023.1.53

С. О. Лисенко
доктор юридичних наук, професор,
завідувач кафедри правознавства
Сєвєродонецького інституту ПрАТ «Вищий навчальний заклад
«Міжрегіональна Академія управління персоналом»
ORCID ID: 0000-0002-7050-5536

РОЗВИТОК СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА СУЧАСНОМУ ЕТАПІ

Стаття присвячена дослідженню розвитку державної системи управління інформаційною безпекою в контексті сучасних викликів і можливостей. Висвітлено вплив технологічного прогресу, геополітичної напруженості та зростаючої залежності від цифрової інфраструктури, підкреслюється важливість надійних механізмів державного управління для забезпечення національної стійкості до кіберзагроз. Особливу увагу виділено законодавчій та інституційній базі в Україні, висвітлюючи досягнутий прогрес та визначаючи прогалини, які потребують уваги для приведення у відповідність до міжнародних стандартів та найкращих практик.Сформульовано ключові компоненти ефективної державної системи інформаційної безпеки, включаючи вдосконалення законодавства, інституційне зміцнення та інтеграцію інноваційних технологій, таких як штучний інтелект та аналітика великих даних. Підкреслено важливість державно-приватного партнерства та міжнародної співпраці як критично важливих елементів для посилення спроможності реагувати на кібервиклики. Ці партнерства і альянси сприяють обміну знаннями, доступу до передових інструментів і єдиних стратегій протидії транснаціональним загрозам.Проаналізовано зростаючу загрозу від дезінформаційних кампаній, які часто організовуються з метою маніпулювання громадською думкою, поляризації суспільств і підриву довіри до демократичних інститутів. У статті виокремлено необхідність комплексних освітніх і просвітницьких програм, спрямованих на подолання людської вразливості у сфері кібербезпеки. Досліджено критичну роль захисту інформаційної інфраструктури в життєво важливих секторах, таких як енергетика, фінанси та охорона здоров'я, для запобігання каскадного впливу на національну безпеку.Розглянуто перспективи подальшого розвитку системи державного управління у сфері інформаційної безпеки з акцентом на гармонізації національних практик зі світовими стандартами. Рекомендації включили в себе стимулювання інновацій, підвищення рівня освіти та впровадження передових моделей управління. Результати дослідження посприяли розумінню стратегій управління інформаційною безпекою на державному рівні та пропонують шлях для побудови стійкої та адаптивної системи для захисту національних інтересів та сприяння сталому розвитку.

Ключові слова: *інформаційна безпека, державне управління, кібербезпека, дезінформація, критична інформаційна інфраструктура, законодавча база, міжнародна співпраця, державно-приватне партнерство, цифрова стійкість, штучний інтелект, кіберзагрози, національна безпека, інституційне зміцнення.*

Актуальність теми дослідження. Поширення інформаційно-комунікаційних технологій (ІКТ) трансформувало майже кожен аспект людської діяльності, сприяючи інноваціям, економічному розвитку та соціальному зв'язку. Однак ця трансформація також призвела до значних вразливостей, включаючи кібератаки, витоки даних, дезінформаційні кампанії та інші загрози, пов'язані з інформацією, які створюють виклики національній безпеці та суспільній довірі.

В умовах геополітичної напруженості та зростаючої залежності від цифрової інфраструктури інформаційна безпека стала запорукою безпеки держави. Гібридна війна, кібершпигунство та використання інформації як зброї стали критичними

викликами для держав у всьому світі. Україна, зокрема, стикається з постійними загрозами для свого інформаційного простору, включаючи спроби дестабілізувати країну через дезінформацію, втручання в критичну інфраструктуру та кіберагресію. Ситуація яка відбувається зараз підкреслю важливість розвитку надійної та адаптивної системи державного управління інформаційною безпекою для захисту національних інтересів та забезпечення стійкості суспільства.

Оскільки нові технології, такі як штучний інтелект і квантові обчислення, продовжують з'являтися, вони створюють як можливості для посилення інформаційної безпеки, так і ризики створення нових вразливостей. Таким чином, існує нагальна потреба в модернізації систем державного управління, щоб привести їх у відповідність до цих технологічних розробок і пом'якшити потенційні ризики.

Мета дослідження — проаналізувати поточний стан системи державного управління інформаційною безпекою, виявити існуючі прогалини та виклики, а також запропонувати рекомендації щодо її вдосконалення у відповідь на еволюцію цифрових загроз.

Аналіз останніх досліджень і публікацій. Результати проведеного аналізу досліджень і публікацій свідчать про зростаючий науковий і практичний інтерес до сфери управління інформаційною безпекою. Науковці широко досліджують роль державного управління, вплив еволюції кіберзагроз, а також необхідність законодавчих та інституційних реформ (Білко С., Малахов Г. Б., Гетьманчук М., Зазуляк З., Бірюков Д. С., Кондратов С. І., Калініченко Б. М., Тєтєвін М. С., Jakobsson M.,). Публікації підкреслюють важливість міжнародної співпраці, технологічних інновацій та освіти у вирішенні поточних проблем. Однак прогалини в дослідженнях відкривають можливості для подальшого вивчення комплексних стратегій.

Основний зміст дослідження. Сучасний стан державного управління інформаційною безпекою в Україні відображає як значний прогрес, так і суттєві виклики у протидії швидкозмінному ландшафту цифрових загроз. Законодавча база слугує фундаментом для національних зусиль із забезпечення інформаційної безпеки, забезпечуючи правову основу для управління ризиками та протидії кіберзагрозам. Серед ключових нормативно-правових актів у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України» [1], який встановлює основи державної політики у сфері кібербезпеки та розмежовує обов'язки різних державних органів. Крім того, Доктрина інформаційної безпеки України [2], затверджена Указом Президента, визначає стратегічні пріоритети захисту національного інформаційного простору від зовнішніх і внутрішніх загроз, включаючи дезінформацію та несанкціонований доступ до критично важливих інформаційних систем.Ці правові інструменти доповнюються галузевими нормативно-правовими актами, спрямованими на захист критичної інфраструктури, захист персональних даних та боротьбу з кіберзлочинністю. Однак залишаються прогалини в гармонізації українського законодавства з міжнародними стандартами та практиками, що розвиваються. Відповідність міжнародно визнаним стандартам, таким як ISO/IEC 27000 серії про системи управління інформаційною безпекою [3], та рекомендаціям таких організацій, як НАТО, стає все більш життєво важливою. Прагнення України поглибити інтеграцію з євроатлантичними структурами спонукає до зусиль, спрямованих на приведення заходів з інформаційної безпеки у відповідність до стандартів НАТО. Включно прийняття керівних принципів з кіберзахисту, розбудови стійкості та обміну інформацією. Незважаючи на досягнутий прогрес, імплементація цих стандартів часто стикається з браком ресурсів, інституційною фрагментацією та обмеженою технічною експертизою.Інституційний механізм управління державною інформаційною безпекою в Україні охоплює низку державних та недержавних структур, завданням яких є забезпечення стійкості національного інформаційного середовища [4]. Рада національної безпеки і оборони України відіграє центральну роль у координації зусиль різних секторів та розробці стратегічної політики у сфері кібербезпеки та інформаційної

безпеки. Державна служба спеціального зв'язку та захисту інформації України відповідає за технічний нагляд, включаючи захист державних систем зв'язку та критичної інфраструктури. Служба безпеки України зосереджується на контррозвідувальних операціях, протидії кібершпигунству та пом'якшенні наслідків дезінформаційних кампаній, спрямованих проти національних інтересів.Незважаючи на дані інституційні зусилля, залишаються значні проблеми. Координація між державними органами часто ускладнюється через дублювання мандатів і недостатню міжвідомчу комунікацію. Така фрагментація може призвести до неефективності реагування на складні кіберінциденти, які потребують комплексного підходу. Крім того, роль приватного сектору та організацій громадянського суспільства у підтримці інформаційної безпеки використовується недостатньо. Приватні компанії, особливо ті, що працюють у технологічному секторі та секторі критичної інфраструктури, є ключовими зацікавленими сторонами у підтримці кіберстійкості. Державно-приватне партнерство, яке є основою ефективного управління інформаційною безпекою в багатьох розвинених країнах, ще не повністю інституціоналізоване в Україні [5]. Так само організації громадянського суспільства відіграють важливу роль у підвищенні обізнаності про цифрову грамотність, боротьбі з дезінформацією та сприянні прозорості державної політики у сфері інформаційної безпеки.

У багатьох розвинених країнах співпраця між урядом і приватним сектором є основою ефективної стратегії інформаційної безпеки. Приватні компанії часто є власниками та операторами значної частини об'єктів критичної інфраструктури, а їхній досвід та ресурси можуть доповнити зусилля уряду. В Україні розвиток таких партнерств має важливе значення для подолання прогалин у спроможності та забезпечення скоординованої відповіді на кіберзагрози. Такі ініціативи, як спільні робочі групи з кібербезпеки, платформи для обміну інформацією та спільні навчальні програми можуть сприяти такій співпраці. Державно-приватне партнерство також може сприяти впровадженню передових практик і стандартів у різних галузях, підвищуючи загальну стійкість національної інформаційної екосистеми.

Виклики та загрози інформаційній безпеці держави на сучасному етапі є багатогранними і зумовлені складною взаємодією технологічних, політичних та суспільних чинників. Серед найбільш значущих викликів - кібератаки та гібридна агресія, які стали визначальними рисами сучасних конфліктів та безпекових дилем. Кібератаки, часто спонсоровані державою, націлені на критичні інформаційні системи, порушують надання основних послуг і підривають цілісність операцій державного і приватного секторів. Гібридна агресія, яка поєднує кібероперації зі звичайними та нетрадиційними тактиками ведення війни, має дестабілізувати держави, використовуючи вразливі місця в їхньому цифровому та інформаційному просторах [6]. В Україні цей виклик є особливо гострим через постійну геополітичну напруженість, що робить країну частою мішенню для кібершпигунства, атак з вимогами викупу та дезінформаційних кампаній.

Захист критичної інформаційної інфраструктури КІІ є ще одним важливим викликом. КІІ охоплює такі сектори, як енергетика, фінанси, охорона здоров'я та транспорт, діяльність яких значною мірою залежить від цифрових систем. Будь-яке порушення роботи цих інфраструктур може мати каскадний вплив на національну безпеку та економіку. Однак забезпечення безпеки є складним завданням, яке вимагає комплексного підходу, що включає оцінку ризиків, моніторинг у режимі реального часу та впровадження надійних механізмів захисту [7]. В Україні відсутність єдиної системи захисту в поєднанні з недостатнім дотриманням існуючих нормативно-правових актів посилює ризики. Крім того, багатьом операторам бракує технічних можливостей та ресурсів для впровадження передових заходів кібербезпеки, що робить критичні системи вразливими до складних атак.

Однією з найгостріших проблем у сфері інформаційної безпеки є недостатнє фінансування та низький рівень технічного оснащення державних органів та інших

зацікавлених сторін. Швидка еволюція кіберзагроз вимагає постійних інвестицій у новітні технології, навчальні програми та модернізацію інфраструктури. Однак бюджетні обмеження часто обмежують можливості держав виділяти адекватні ресурси на інформаційну безпеку. В Україні пріоритетність інших нагальних питань, таких як відновлення економіки та витрати на оборону, ще більше обмежила виділення коштів на ініціативи з кібербезпеки. Цей дефіцит фінансування ускладнюється обмеженою кількістю кваліфікованих фахівців з кібербезпеки, що перешкоджає ефективному впровадженню політики і стратегій безпеки.

Вплив дезінформації на громадську думку є зростаючою загрозою у сфері інформаційної безпеки. Дезінформаційні кампанії, які часто координуються іноземними суб'єктами, спрямовані на маніпулювання громадською думкою, поляризацію суспільства та підрив довіри до демократичних інститутів. Дані кампанії використовують платформи соціальних мереж, інтернет-видання та інші цифрові канали для масового поширення неправдивої або оманливої інформації [8]. Виклик полягає не лише у виявленні та протидії дезінформації, а й в усуненні її першопричин, таких як брак цифрової грамотності та навичок критичного мислення серед населення в цілому. В Україні дезінформація використовується як інструмент для використання суспільних розбіжностей та підриву довіри громадян до здатності уряду ефективно врегульовувати кризові ситуації.

Перспективи розвитку системи державного управління у сфері інформаційної безпеки нерозривно пов'язані з вирішенням сучасних викликів та приведенням національної практики у відповідність до світових стандартів та інновацій. Фундаментальним пріоритетом є вдосконалення законодавчої бази, яка слугує основою для ефективного управління та механізмів реагування. Сучасні нормативно-правові акти, що регулюють питання кібербезпеки, захисту персональних даних та захисту критичної інформаційної інфраструктури, є необхідними для створення надійного правового середовища. В Україні було досягнуто значних успіхів у прийнятті ключових законодавчих заходів, але для того, щоб не відставати від швидкої еволюції загроз у цифровій сфері, необхідне їх подальше вдосконалення та адаптація. Комплексне законодавство має усунути прогалини, пов'язані з класифікацією кіберінцидентів, відповідальністю за кіберзлочини та механізмами міжнародного співробітництва.

Інтеграція з міжнародними ініціативами є ще однією важливою сферою розвитку в контексті забезпечення інформаційної безпеки. Участь у глобальних альянсах, спрямованих на протидію кіберзагрозам, таких як партнерство з Європейським Союзом, НАТО та іншими міжнародними організаціями, посилює спроможність національних систем ефективно реагувати на складні кібервиклики [9]. Ця співпраця сприяє обміну розвідданими, передовим досвідом і технологічними інструментами, створюючи єдиний фронт протидії транснаціональним загрозам. Для України поглиблення зв'язків з міжнародними партнерами також слугує ширшій меті - привести свою практику інформаційної безпеки у відповідність до євроатлантичних стандартів, тим самим зміцнюючи своє геополітичне позиціонування.

Роль інновацій у розвитку системи державного управління важко переоцінити, оскільки нові технології, такі як штучний інтелект, машинне навчання та аналіз великих даних, мають трансформаційний потенціал для сфери інформаційної безпеки. Інструменти на основі штучного інтелекту можуть покращити виявлення загроз і час реагування на них, аналізуючи величезні масиви даних у режимі реального часу, виявляючи аномалії та прогнозуючи потенційні порушення безпеки. Аналогічно, аналітика великих даних дозволяє політикам отримати уявлення про кібер-тенденції, оцінити ризики і сформулювати стратегії, засновані на даних. Однак інтеграція цих технологій у державне управління вимагає значних інвестицій, розбудови потенціалу та підготовки кваліфікованої робочої сили, здатної ефективно використовувати ці інструменти.

Освіта та підвищення обізнаності громадськості є невід'ємними компонентами

стійкої системи інформаційної безпеки, тому людський фактор часто є найслабшою ланкою кібербезпеки, оскільки люди вразливі до фішингових атак, дезінформації та інших маніпулятивних тактик [10]. Підвищення цифрової грамотності та обізнаності щодо кібербезпеки серед громадян, державних службовців та працівників приватного сектору є важливим для зменшення цієї вразливості. Освітні програми, громадські кампанії та навчальні ініціативи мають бути спрямовані на популяризацію безпечної поведінки в Інтернеті, розпізнавання кіберзагроз та розуміння наслідків порушення цифрової приватності. Крім того, інтеграція освіти з кібербезпеки в навчальні програми на всіх рівнях забезпечує розвиток цифрово грамотного покоління, здатного зробити свій внесок в інформаційну безпеку країни.

Перспективи розвитку системи державного управління у сфері інформаційної безпеки залежать від багатогранного підходу, який охоплює вдосконалення законодавства, міжнародну співпрацю, технологічні інновації та освіту населення. Звертаючись до цих сфер, Україна може побудувати стійку та адаптивну систему інформаційної безпеки, яка не лише захистить її національні інтереси, але й позиціонуватиме її як проактивного учасника глобальної екосистеми кібербезпеки. Комплексна стратегія має вирішальне значення для захисту суверенітету країни, зміцнення довіри до державних інституцій та забезпечення сталого розвитку у все більш взаємопов'язаному світі.

Крім того, зростає потреба в посиленні інституційної спроможності органів державного управління, відповідальних за інформаційну безпеку. Це передбачає не лише оснащення цих установ сучасними технологіями, а й розвиток культури адаптивності та інновацій. Створення спеціальних підрозділів з реагування на кібератаки, посилення міжвідомчої координації та забезпечення можливостей безперервного професійного розвитку для державних службовців є критично важливими кроками. Крім того, інтеграція досліджень і розробок (R&D) в систему державного управління може стимулювати створення власних рішень у сфері кібербезпеки, адаптованих до конкретних викликів, з якими стикається країна.

Висновки та перспективи подальших досліджень. Розвиток надійної системи державного управління інформаційною безпекою є критично важливим пріоритетом в епоху стрімкого технологічного прогресу та зростання цифрових загроз. У цій статті підкреслюється важливість комплексного підходу до вирішення ключових проблем, таких як кібератаки, захист критичної інформаційної інфраструктури, недостатнє фінансування та повсюдний вплив дезінформації на громадську думку. Аналіз підкреслює необхідність багатогранної стратегії, яка включає вдосконалення законодавства, розбудову інституційної спроможності, технологічні інновації та просування цифрової грамотності. Інтеграція в міжнародні ініціативи та альянси, в тому числі партнерство з Європейським Союзом і НАТО, стала життєво важливим компонентом для посилення національної стійкості до кіберзагроз. Така участь сприяє обміну знаннями, доступу до передових технологій та розробці єдиних стратегій протидії транснаціональним кібервикликам.

Перспективи подальших досліджень включають вивчення передових технологічних рішень, таких як штучний інтелект, блокчейн і квантові обчислення, для вдосконалення заходів інформаційної безпеки. Порівняльний аналіз найкращих світових практик управління інформаційною безпекою може надати цінну інформацію про стратегії, які можуть бути адаптовані до українського контексту. Оцінка економічного впливу інвестицій у кібербезпеку може запропонувати політикам рекомендації щодо розподілу ресурсів на основі даних. Вивчення моделей державно-приватної співпраці у сфері інформаційної безпеки може допомогти розробити основи для ефективного партнерства. Крім того, вивчення поведінкових аспектів кібербезпеки, в тому числі психологічних і соціальних факторів, що впливають на сприйнятливість громадськості до кіберзагроз і дезінформації, може підвищити ефективність інформаційних кампаній.

Вивчення децентралізованого управління як потенційного підходу до вдоско-

налення національної системи інформаційної безпеки може призвести до створення більш стійких і адаптивних систем. Звернення до цих дослідницьких напрямків сприятиме розробці інноваційних, стійких і комплексних рішень для подолання викликів, пов'язаних з мінливим цифровим ландшафтом, забезпечуючи захист національних інтересів і сприяючи економічному розвитку, суспільній довірі та міжнародному співробітництву.

Список використаної літератури:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Офіційний веб-портал Верховної Ради України URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України; Доктрина від 25.02.2017 № 47/2017. Офіційний веб-портал Верховної Ради України URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text
3. International Organization for Standardization. (2018). ISO/IEC 27000:2018 Information technology. URL: https://www.iso.org/standard/73906.html
4. Білко, С. Інституційне забезпечення інформаційної безпеки України. Економіка і регіон. 2021. № 3(82). С. 36–41. URL: https://journals-nupp-edu-ua.translate.goog/eir/article/view/2361?_x_tr_sl=uk&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc
5. Заскока Ю.В. Державно-приватне партнерство в сфері кібербезпеки України: стан та проблеми забезпечення. *Наукові перспективи*. 2021. № 9 (15). URL: http://perspectives.pp.ua/index.php/np/article/view/467/470
6. Гетьманчук, М., Зазуляк, З.. Інформаційна сфера - ключовий фактор гібридної агресії Росії проти України. Соціальні комунікації: теорія і практика 2019. № 5(1). С. 7–12. URL: https://doi.org/10.23939/shv2019.01.007
7. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Д. С. Бірюков, С. І. Кондратов. К. : НІСД, 2012. 96 с.
8. Калініченко Б. М. Формування громадської думки, як чинник забезпечення успіху в інформаційній війни. *Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін.* 2020. № 27. С. 69-74. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/29432/Kalinichenko.pdf?sequence=1&isAllowed=y
9. Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade. Council of the European Union. Brussels, 9 March 2021. No 6722/21.
10. Jakobsson M. The Human Factor in Phishing. *Privacy & Security of Consumer Information.* 2007. pp. 1–19. URL: https://markus-jakobsson.com/papers/jakobsson-psci07.pdf

Lysenko S. O. Development of the state information security management system at the present stage

The article is devoted to the study of the development of the state system of information security management in the context of modern challenges and opportunities. The author highlights the impact of technological progress, geopolitical tensions and growing dependence on digital infrastructure, and emphasises the importance of reliable public administration mechanisms to ensure national resilience to cyber threats. Particular attention is paid to the legislative and institutional framework in Ukraine, highlighting the progress made and identifying gaps that need attention to bring them in line with international standards and best practices.The key components of an effective state information security system are outlined, including improved legislation, institutional strengthening, and the integration of innovative technologies such as artificial intelligence and big data analytics. The importance of public-private partnerships and international cooperation as critical elements for strengthening the ability to respond to cyber challenges is highlighted. These partnerships and alliances facilitate the exchange of knowledge, access to advanced tools and common strategies to counter transnational threats.The article analyses the growing threat of disinformation campaigns, which are often organised to manipulate public opinion, polarise societies and undermine trust in democratic institutions. The article highlights the need for comprehensive educational and awareness-raising programmes aimed at overcoming human vulnerability in the field of cybersecurity. The critical role of protecting information infrastructure in vital

sectors such as energy, finance and healthcare is explored to prevent cascading effects on national security. Prospects for further development of the public administration system in the field of information security with a focus on harmonising national practices with international standards are considered. Recommendations included stimulating innovation, raising the level of education and introducing advanced management models. The study's findings contributed to the understanding of information security management strategies at the state level and offer a way forward for building a resilient and adaptive system to protect national interests and promote sustainable development.

Key words: *information security, public administration, cybersecurity, disinformation, critical information infrastructure, legislative framework, international cooperation, public-private partnership, digital resilience, artificial intelligence, cyber threats, national security, institutional strengthening*