Ефективність державного управління
Efficiency of public administration
https://doi.org/10.36930/508206
Article received 15.03.2025
Article accepted 26.06.2025
УДК 351:004.056
Correspondence author: Y. V. Honcharuk honcharuk.yuriy@nltu.lviv.ua
ISSN 2070-4011 (print)
ISSN 2786-6580 (online)

Ю. В. Гончарук
Національний лісотехнічний університет України, м. Львів, Україна

ТРАНСФОРМАЦІЯ ПАРАДИГМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПУБЛІЧНОМУ УПРАВЛІННІ ЧЕРЕЗ ЗРОСТАННЯ ЗАГРОЗ КІБЕРПРОСТОРУ

Розглянуто питання безпеки та захисту інформації як складових частин національної безпеки держави. Безпека держави визначається стійкістю основних сфер життєдіяльності до небезпечних, дестабілізаційних інформаційних впливів стосовно інтересів держави. Стрімкий розвиток інформаційної сфери зумовлює появу принципово нових загроз інтересам суспільства, держави та її національній безпеці. Актуальність проблеми полягає в тому, що інформація є об'єктом маніпуляції за умов воєнного стану. Забезпечення національної безпеки є одним з фундаментальних факторів впливу на діяльність держави з метою усунення загроз шляхом розвитку національної індустрії сучасних інформаційних технологій та впровадження їх у всі сфери життєдіяльності держави та суспільства. Витік інформації загрожує роботі органів влади та критичної інфраструктури, оскільки може бути використаний ворогом для подальших атак.

З'ясовано, що всі інформаційні системи, вимоги до захисту яких закріплено у законодавстві України, мають бути захищені згідно з національними та міжнародними стандартами. Державні інформаційні ресурси потрібно обробляти із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюють за результатами державної експертизи. Таку експертизу проводять з урахуванням галузевих вимог і норм інформаційної безпеки.

Акцентовано увагу на тому, що захист інформації – це процес забезпечення конфіденційності, цілісності і доступності даних та інформаційних ресурсів. Це охоплює різноманітні заходи та технології, спрямовані на захист інформації від несанкціонованого доступу, модифікації, втрати, знищення. Здійснено аналіз кіберзлочинів під час воєнного стану. Запропоновано розглядати інформаційну безпеку та захист інформації як комплекс заходів, спрямованих на забезпечення безпеки держави в інформаційному просторі, а також на захист інформації від незаконного доступу, використання.

Ключові слова: інституційне забезпечення національної системи кібербезпеки; державна безпека; інформаційна безпека; інформація; кібербезпека; кіберзлочини; кібертероризм; хакерські атаки.

Вступ

Державна безпека тісно пов'язана із захистом інформації. Інформаційна безпека держави означає, що життєво важливі інтереси як окремої людини, так і всього суспільства та держави перебувають під надійним захистом в інформаційному просторі. Ключову роль у забезпеченні інформаційної безпеки держави відіграє цілеспрямована діяльність органів, які використовують спеціальні засоби для захисту інформаційного середовища, що є критично важливим для ефективного функціонування та розвитку країни та суспільства.

Після повномасштабного вторгнення Росії значення інформаційної безпеки зростає. Російські хакери намагаються пошкодити українські інформаційні системи та отримати доступ до особистих даних громадян України. Ці дії поєднуються з регулярними нападами на критичну інфраструктуру. До початку повномасштабного вторгнення Росії українські інформаційні системи вже зазнавали потужних атак з боку російських хакерів. Проте з початком повномасштабної агресії Росії їх інтенсивність ще більше зросла. Витік інформації та пошкодження ключових інформаційних ресурсів може серйозно загрожувати функціонуванню державних органів та критичної інфраструктури, оскільки ворог може використати її для подальших атак. Кібератаки на Україну посилилися у 2024 р., збільшившись майже на 70 %, порівняно з 2023 р. [1]. Найчастіше хакери атакують критично важливу інфраструктуру: енергетичний сектор, урядові установи, органи безпеки та телекомунікації. Їх метою є викрадення чутливої інформації та знищення даних.

Під час війни найціннішою для ворога є інформація про плани сил оборони України, дані підприємств оборонно-промислового комплексу, уряду та інших організацій, які здійснюють підтримку військових. Кібервійна залишається одним із ключових інструментів РФ для дестабілізації ситуації в Україні. У 2024 р. спостерігали стійку тенденцію до зростання атак на критичну інфраструктуру, особливо в енергетиці [1].

У грудні 2024 р. було здійснено одну з наймасштабніших кібератак на державні реєстри України. Як наслі-

Інформація про авторів:
Гончарук Юрій Володимирович, аспірант кафедри публічного управління та адміністрування.
Email: honcharuk.yuriy@nltu.lviv.ua; https://orcid.org/0009-0000-0314-1579

Цитування за ДСТУ: Гончарук Ю. В. Трансформація парадигми інформаційної безпеки в публічному управлінні через зростання загроз кіберпростору. *Ефективність державного управління* : зб. наук. пр. Вип. 1/2(82/83). Львів: НЛТУ України, 2025. С. 47–52.

Citation APA: Honcharuk, Y. V. (2025). The evolution of the information security paradigm in public management as cyberspace threats proliferate. *Efficiency of public administration, 1/2*(82/83), 47–52. https://doi.org/10.36930/508206

док, було тимчасово паралізовано роботу Єдиних та Державних реєстрів, які перебувають у компетенції Міністерства юстиції України, зокрема Державного реєстру актів цивільного стану громадян, Державного реєстру прав на нерухоме майно, Єдиного реєстру довіреностей, завірених у нотаріальному порядку та багато інших [1]. Як наслідок, на певний час громадяни не могли здійснювати такі важливі операції як оформлення угод купівлі-продажу рухомого та нерухомого майна, актів цивільного стану, довіреностей та багато інших.

У цьому контексті захист даних в інформаційних системах є дуже актуальною сучасною проблемою

Методи та інформаційна база дослідження

Методологічною основою дослідження є загальнофілософські, загальнонаукові та спеціальні методи пізнання явищ і процесів у системі інформаційної безпеки. Вивчення термінологічної бази, функцій, законів, національних і міжнародних стандартів стосовно захисту інформації здійснено на основі використання методів класифікації, теоретичного узагальнення, спостереження, аналогії. Для визначення сучасного стану боротьби з кіберзлочинами було застосовано методи статичного спостереження, групування, аналіз та синтез.

Інформаційною базою для дослідження стали звіти Оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку, наукові публікації та матеріали ЗМІ.

Аналіз останніх досліджень і публікацій

Питання безпеки та захисту інформації розглядали О.В. Федорчук [19], В.І. Франчук [20], І. Жданов [12], О.С. Кириченко [14], Т.В. Субіна [18], Б.А. Кормич [16] та інші. У цих працях переважно досліджують загальнотеоретичні питання інформаційної безпеки і захисту інформації окремих органів влади. Проте вони не враховують останніх тенденцій щодо зростання кібератак на Україну. Окрім цього, наявні праці недостатньо розкривають способи перевірок систем інформаційної безпеки органів державної влади.

Мета дослідження та основні завдання для її досягнення. Метою дослідження є вивчення тенденцій змін у процесах гарантування інформаційної безпеки через зростання загроз кіберпростору за умов повномасштабного вторгнення з боку Росії, що зумовило основні завдання дослідження:

- систематизувати теоретичні положення і сформулювати основні поняття, що характеризують інформаційну та кібербезпеку;
- окреслити основні засоби і методичні способи захисту інформації;
- визначити можливі методичні способи для перевірки системи інформаційної безпеки органу державної влади;
- аргументувати можливі шляхи підвищення рівня інформаційної безпеки в органах державної влади.

Виклад основного матеріалу дослідження з обґрунтуванням одержаних результатів

У сучасному світі існує величезне розмаїття загроз безпеці, які можуть впливати на окрему людину, суспільство та державу загалом. Ці загрози охоплюють широкий спектр сфер: від непередбачуваних природних катаклізмів і складних техногенних аварій до комплексних соціальних викликів, таких як тероризм і внутрішні конфлікти. Особливого значення набувають кіберзагрози, що виникають у високотехнологічному світі, а також економічні ризики, які можуть підірвати стабільність будь-якої країни. Розуміння поняття безпеки є критично важливим для ефективного захисту та забезпечення стабільного розвитку.

Поняття «безпека» є багатозначним і використовується в різних сферах діяльності – від особистого життя до державного управління, інформаційних технологій, екології, економіки тощо. На думку І. Коржа, воно означає складне соціально-політичне явище, оскільки акумулює в собі багатогранну життєдіяльність, набутий історичний досвід, уподобання і культуру кожної людини, суспільства держави, загалом земної цивілізації [15]

Зважаючи на особливу актуальність, у нашому дослідженні ми зосередимося на взаємозв'язку національної, державної та, особливо, інформаційної безпеки.

Згідно із законом України «Про національну безпеку України»: «Національна безпека України – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [10]. Вона охоплює воєнну, політичну, міжнародну, інформаційну, економічну, соціальну, енергетичну та екологічну складові.

Державна безпека, як визначальна складова частина національної безпеки – це «захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру» [10]. У статті 17 Конституції України зазначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Оборона України, захист її суверенітету, територіальної цілісності і недоторканності покладаються на Збройні Сили України. Забезпечення державної безпеки і захист державного кордону України покладаються на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом» [9].

Перш ніж заглибитись у сутність інформаційної безпеки, потрібно чітко визначити саме поняття "інформація", що означає «відомості про які-небудь події, ситуації, чиюсь діяльність» [11, с. 282]. Інформацію у правовому аспекті розуміють як «будь-які відомості та/або дані, які мають бути збережені на матеріальних носіях або відображені в електронному вигляді (ст. 1 Закону України «Про інформацію»)» [21, с. 355]. За нинішніх умов інформація є надзвичайно цінним активом, і будь-яке несанкціоноване заволодіння нею, порушення її цілісності або повне руйнування може завдати непоправної шкоди, що робить інформаційну безпеку критично важливим поняттям для захисту цих життєво важливих даних. Визначення "інформаційної безпеки" по-різному трактують науковці. Детальний огляд цих визначень подано у табл. 1.

Термін «Інформаційна безпека (Information Security)» згідно з міжнародними стандартами ISO визначається як забезпечення конфіденційності, цілісності та доступності інформації [3]. У стандартах ISO/IEC 13335-1 та ISO/IEC 27001 до цього визначення до-

дається забезпечення таких властивостей інформації як облік, достовірність та надійність [3]. Наголошено, що інформаційна безпека не є статичним поняттям, а динамічно змінюється. Її рівень визначається різними властивостями інформації в конкретний момент часу. Така мінливість зумовлена непостійністю характеристик інформації та коливанням числа активних зовнішніх і внутрішніх загроз.

Табл. 1. Визначення поняття інформаційна безпека у працях науковців

Автори та назви джерел	Визначення
Федорук О.В. [19]	Під державно-правовим механізмом інформаційної безпеки розуміють систему дії державно-правових інститутів, діяльність яких спрямована на створення умов для ефективної реалізації інформаційної політики держави.
Франчук В. І. [20]	Основними заходами із забезпечення інформаційної безпеки держави є юридичні, організаційно-економічні та технологічні заходи, що ґрунтуються на засадах: створення нормативно-правової бази інформаційних відносин у суспільстві.
Жданов І. [12]	Достатній рівень захищеності інформаційної інфраструктури та інформаційних ресурсів може бути досягнутий унаслідок забезпечення надійного функціонування державних та суспільних інститутів з метою реалізації практичних заходів із забезпечення інформаційної безпеки.
Кириченко О.С. [14]	Пріоритетними напрямами у забезпеченні інформаційної безпеки держави є формування стратегії, вдосконалення інформаційної політики держави, підвищення інтелектуального, наукового, технічного, технологічного рівня інтелектуальних інформаційних продуктів, баз даних та систем із метою рівноправної інтеграції країни в міжнародний інформаційний ринок, реалізація національних інтересів в інформаційній сфері.
Субіна Т.В. [18]	Інформаційна безпека в податкових органах – це система унормованих методів, заходів, засобів дотримання належного рівня охорони і захисту інформації та недопущення негативного інформаційного впливу на діяльність податкової служби.
Кормич Б.А. [16]	Забезпечення інформаційної безпеки має здійснюватися шляхом виваженої і збалансованої політики держави в інформаційній сфері.
Остроухов В., Петрик В. [17]	Інформаційна безпека – це стан захищеності об'єкта, за якого досягається його нормальне функціонування незалежно від зовнішніх і внутрішніх інформаційних впливів.
І. Зайцева-Калаур [13]	Поєднує інформаційної безпеку особистості та суспільства, оскільки інформаційна безпека окремої особистості формує у кінцевому підсумку інформаційну безпеку суспільства та держави.
М. Яблонський і М. Мелус [4]	Передбачає низку заходів, яких потрібно вжити, щоб отримати бажаний стан безпеки (запобігання (профілактика), відлякування, індикація і застереження, виявлення, підготовка до надзвичайної ситуації і реакція на можливі атаки).

Примітка: складено за даними наведених авторів.

На наш погляд, інформаційна безпека є набагато ширшим поняттям, що визначає комплекс заходів, спрямованих на захист інформації громадянина, суспільства та держави від несанкціонованого доступу, використання, розголошення, руйнування, ознайомлення або знищення і спрямована на забезпечення конфіденційності, цілісності і доступності, гарантування її безпечного зберігання, обробки та передавання.

Захист інформації, як складова інформаційної безпеки, може охоплювати як технічні, так і організаційні засоби, такі як:

- фізичний захист (механізми обмеження доступу до приміщень, системи відеомоніторингу (CCTV), фізична охорона у приміщенні тощо);
- правові аспекти (нормативно-правові акти, політики та процедури, які встановлюють правила роботи інформацією на рівні державних інституцій та органів місцевого самоврядування тощо);
- програмно-технічні засоби захисту інформації (антивіруси, операційні системи, спеціалізоване ПЗ для створення резервних копій тощо).

У кожній країні існують нормативно-правові акти, що охоплюють різні аспекти інформаційної безпеки:

- закони, урядові правила та положення. Наприклад, SOX (Sarbanes-Oxley, 2002) про управління та фінансове управління підприємствами та HIPAA (Закон про мобільність та підзвітність медичного страхування, 1996) про захист особистої інформації для медичного використання;
- національні стандарти: у більшості країн є організація, відповідальна за розробку та розповсюдження національних стандартів. Ці національні стандарти можуть бути обов'язковими чи добровільними. У деяких випадках обов'язкові стандарти мають чинність закону, як і інші технічні регламенти. Наприклад, NIST 800-53 (США) містить рекомендації щодо безпеки інформаційних систем у державному секторі [7].
- міжнародні стандарти: більшість міжнародних стандартів, таких як ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO 22301 [3] тощо. Проте існує кілька інших стандартів, розроблених іншими міжнародними організаціями, такими як Організація економічного співробітництва та розвитку (OECP).

Зазначені вище нормативно-правові документи встановлюють вимоги до побудови систем інформаційної безпеки. Проте іншим важливим аспектом є забезпечення їхньої ефективності. Для цього необхідно їх регулярно перевіряти, використовуючи різноманітні методичні способи.

Методичні способи для перевірки системи інформаційної безпеки органів державної влади наведено у табл. 2.

На основі результатів вказаних вище перевірок або аудитів можна оцінити ступінь дотримання вимог, встановлених нормативно-правовими документами. Наступним кроком буде усунення відхилень, виявлених під час таких процедур. Але перевірки проводять не завжди, а системи інформаційної безпеки важливо постійно підтримувати у стані готовності протидії актуальним загрозам. З огляду на це для забезпечення захисту інформації потрібні також:

- постійна технічна підтримка комп'ютерних систем, мереж та інформаційних технологій від кібератак, вірусів, хакерських атак та інших загроз кібернетичної безпеки;

- моніторинг потенційних маніпуляцій, фальсифікацій та інших видів зловживання;
- використання сучасних криптографічних методів (шифрування) для захисту конфіденційної інформації від несанкціонованого доступу;
- регулярне підвищення обізнаності та навичок у громадян щодо безпеки в Інтернеті та користування інформаційними технологіями;
- співпраця з іншими країнами та міжнародними організаціями у сфері кібербезпеки та захисту інформації для обміну інформацією.

Табл. 2. Методичні способи для перевірки системи інформаційної безпеки органу державної влади

№ з/п	Джерела інформації	Характеристика
1	Спостереження	Спостереження, що серверна кімната дійсно заблокована механізмом доступу на магнітній карті (RFID)
2	Конфігурації системи	Конфігурації брандмауера, демонструють, що доступ до шкідливих вебсайтів заблоковано
3	Індикатори	Інформаційні панелі щодо індикаторів інцидентів безпеки
4	Бази даних і вебсайти	База даних співробітників організацій та інтернет
5	Записи	Журнали доступу до серверної кімнати, відвантаженої системою доступу до магнітних карт, журнал постів тощо
6	Документи	Політика безпеки, процедура встановлення програмного забезпечення, керівництво для співробітників, звіти з інших джерел (наприклад, зовнішні питання та виміри) та ін.
7	Інтерв'ю	Інтерв'ю з адміністратором мережі, групове інтерв'ю з персоналом.

Примітка: складено на основі [13].

Невід'ємним елементом інформаційної безпеки, важливість якого стрімко зростає разом з цифровізацією суспільства, є кібербезпека – це частина захисту інформації, яка зосереджується на безпеці інформаційних систем і мереж у цифровому середовищі. Кібербезпека виявляє такі загрози, як: [3]

- хакерські атаки;
- шкідливе програмне забезпечення;
- фішинг;
- витік даних у кіберпросторі;
- DDoS-атаки;
- скінінг;
- кібершпигунство тощо

Кібербезпека – вузька галузь, яка спеціалізується саме на цифрових технологіях і протидії кіберзагрозам. Якщо конфіденційний документ зберігається у сейфі, його захист – це захист інформації. Якщо цей документ розміщений у комп'ютерній мережі, то його захист вже входить до сфери кібербезпеки.

За інституційне забезпечення національної системи кібербезпеки відповідає Державна служба спеціального зв'язку та захисту інформації України. Вона координує роботу всіх суб'єктів, що забезпечують кібербезпеку в напрямі кіберзахисту, а також виконує функції адміністратора зв'язку. Ця служба є спеціалізованим органом центральної виконавчої влади у галузі спеціального зв'язку та захисту інформації, є суб'єктом сектору оборони і безпеки відповідно до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» [8].

Коли йдеться про Україну, то воєнні дії є ще одним важливим чинником, який вимагає швидкого впровадження нових технологій для відповіді новим викликам. Під час їхнього впровадження, потрібно, щоб часові межі не були надто стислими для впровадження належних заходів кібербезпеки, а також знати, чи достатньо вони захищені від нових стратегій хакерів.

Під час роботи з конфіденційною та таємною інформацією публічні управлінці зобов'язані гарантувати її безпеку від будь-якого несанкціонованого втручання, такого як ознайомлення, зміна, знищення, копіювання чи поширення без дозволу. Доступ до цих даних мають отримувати лише ті користувачі, чия особа встановлена. Будь-які спроби доступу неідентифікованих осіб повинні бути негайно припинені.

Підхід органів державної влади до захисту інформації має бути комплексним та повинен враховувати специфіку та потреби кожної окремої організації чи установи. Недостатньо просто впровадити загальні заходи захисту. Критично важливо адаптувати їх до конкретного середовища. Органи державної влади, які працюють з конфіденційною інформацією або забезпечують функціонування критично важливих галузей життєдіяльності України (енергетика, фінанси, транспорт, зв'язок тощо), повинні приділяти значно більше уваги та ресурсів кібер- та інформаційній безпеці. Для таких державних інституцій ризики у разі кібератак чи витоку даних є набагато вищими, адже вони можуть призвести до серйозних соціальних, економічних чи навіть національних катастроф. Тому їхні системи захисту мають бути не просто надійними, а надзвичайно стійкими та еластичними, здатними протистояти найскладнішим кіберзагрозам і швидко відновлюватися після інцидентів. Це вимагає постійного моніторингу, регулярних аудитів безпеки, навчання персоналу та впровадження передових технологій захисту.

З огляду на статистику можна констатувати невпинне зростання потреби у сучасних інформаційних засобах. Державний центр кіберзахисту, який функціонує у складі Державної служби спеціального зв'язку та захисту інформації України, у 2022 р. зареєстрував у 2,8 раза більше кіберінцидентів, ніж у 2021 році. У 2023 р. кількість зареєстрованих кіберінцидентів зросла на 62,5 %, порівняно з 2022 р. [3].

У табл. 3 наведено аналіз кіберзлочинів за два роки війни.

У 2024 р. кількість кібератак на Україну зросла ще більше – на 69,8 %, досягнувши 4315 інцидентів, порівняно з 2023 р., коли було зафіксовано 2541 кіберінциденти [2].

Усі ці дані свідчать про нагальну потребу посилення ролі захисту інформації у всіх сферах, оскільки ми спостерігаємо стійкий тренд на зростання кібератаки щодо України. Плюс не варто забувати, що всі процеси

в Україні рухаються в напрямі цифровізації, що може ще більше мультиплікувати ризики.

Табл. 3. Аналіз кіберзлочинів у період воєнного стану

Кіберінциденти	2022	2023
Опрацьовано подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки	58 млрд	18 млрд
Детектовано підозрілих подій інформаційної безпеки (за первинного аналізу)	182 млн	133 млн
Опрацьовано критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу)	179 тис.	148 тис.
Зафіксовано та оброблено безпосередньо аналітиками безпеки кіберінцидентів (критичних подій ІБ).	415	1105
Підключено нових об'єктів кіберзахисту з урядового, енергетичного та військового секторів	13	24

Примітка: складено за даними [7].

Висновки та перспективи подальших розвідок

В Україні існує критична потреба у державному регулюванні науково-технічної та інформаційної сфер, яке б відповідало сучасним тенденціям розвитку інформаційних технологій та міжнародним правовим стандартам, але при цьому дієво захищало національні інтереси. За сучасних умов розбудова ефективних систем кібербезпеки є важливим елементом функціонування інформаційних систем. Сьогодні інформаційна складова національної безпеки є надзвичайно значущою через наявні поширені види загроз, такі як кібертероризм, кіберзлочинність, агресивна пропаганда, поширення антидержавних ідей, обмеження доступу населення до публічної інформації та інше.

Посилення інформаційної безпеки в державі потребує комплексного підходу на рівні законодавства, технологій, освіти та міжнародної співпраці.

Для цього необхідно:

- приведення законів у відповідність до сучасних викликів кібербезпеки (включно з обороною від гібридної агресії);
- обов'язкові стандарти кіберзахисту для державних установ, критичної інфраструктури та бізнесу.
- введення суворої відповідальності за кібератаки, фішинг, дезінформацію, саботаж тощо.
- забезпечення цілодобового моніторингу, аналізу загроз і швидкого реагування;
- навчання держслужбовців та військових основам кібергігієни та протидії інформаційним атакам;
- створення програм в університетах з кібербезпеки, інфозахисту, OSINT, криптографії тощо.
- аудити безпеки в органах державної влади та критичній інфраструктурі.
- централізоване оновлення програмного забезпечення та захисту в державних установах тощо.

Отже, державна безпека та захист інформації – це комплекс заходів, спрямованих на забезпечення безпеки держави в інформаційному просторі, а також на захист інформації від незаконного доступу, використання або зміни.

References

1. BBC.com (2025). Російські хакери зламали державні реєстри України. URL: https://www.bbc.com/ukrainian/articles/c7ve1298ndgo.amp
2. CIP (2025). CERT-UA минулого року опрацювала 4315 кіберінцидентів. Державна служба спеціального зв'язку та захисту інформації України. 08.01.2025. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
3. ISO (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001
4. Jabłoński, M., & Mielus, M. (2010). Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej, [In:] Bezpieczeństwo informacji i biznesu Zagadnienia wybrane,pod red. Kwieciński M., Oficyna Wydawnicza AFM, Kraków, 11–14.
5. Kost. E. (2023). The 6 Biggest Cyber Threats for Financial Services in 2023. UpGuard: Blog. URL: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services
6. Scarfone Cybersecurity (2012). Керівні настанови щодо управління інцидентами, пов'язаними з комп'ютерною безпекою: NIST SP 800-61 Rev. 2. Національний інститут стандартів і технологій Міністерства торгівлі США; розроб. Scarfone Cybersecurity. Серпень 2012. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
7. SCPC (2023). Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. URL: https://scpc.gov.ua/uk/articles/334
8. Верховна Рада України (2006). Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» №3475-IV від 23.02.2006. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text
9. Верховна Рада України (2013). Конституція України: офіц. текст. Київ: КМ, 96.
10. Верховна Рада України (2024). Закон України «Про національну безпеку України» 2469-VIII від 09.08.2024 URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
11. Єрошенко. О. (2012). Великий тлумачний словник сучасної української мови. Донецьк: ТОВ "Глорія-Трейд", 864.
12. Жданов, І. (2001). Можливі підходи до визначення основ державної політики забезпечення інформаційної безпеки України. *Безпека інформації в інформаційно-телекомунікаційних системах; Матеріали до круглого столу*, 11–19.
13. Зайцева-Калаур, І. В. (2014). Інформаційне право. Тернопіль: ФОП Шпак В.Б., 185.
14. Кириченко, О. С. (2018). Концептуальні засади формування системи забезпечення інформаційної безпеки держави. *Вчені записки Університету «КРОК»*, 49, 19–26. https://doi.org/10.31732/2663-2209-2018-49-19-26
15. Корж, І. І. (2019). Безпека: методологічні підходи до поняття. *Jurnalul juridic național: teorie și practică, 8*, 68–72.
16. Кормич, Б. А. (2004). Інформаційна безпека: Організаційно-правові основи: навчальний посібник. Київ: Кондор, 384.
17. Остроухов, В., & Петрик, В. (2008). До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент, 4*, 135–141. URL: http://nbuv.gov.ua/UJRN/PoMe_2008_4_16
18. Субіна, Т. В. (2009). Забезпечення інформаційної безпеки електронної звітності в органах Державної податкової служби України. *Правова інформатика, 1*(21), 87–93.
19. Федорук, О. В. (2013). Концептуальні засади формування системи забезпечення національної інформаційної безпеки. *Вісник соціально-економічних досліджень, 2*(1), 182–188. URL: http://nbuv.gov.ua/UJRN/Vsed_2013_2%281%29__29
20. Франчук, В. І . (2010). Економічна безпека. Львів: ЛДУВС, 243.
21. Шемшученка. Ю. С. (2012). Великий енциклопедичний юридичний словник. 2nd. ed. Київ: Вид-во "Юридична думка", 1020.

Y. V. Honcharuk
Ukrainian National Forestry University, Lviv, Ukraine

THE EVOLUTION OF THE INFORMATION SECURITY PARADIGM IN PUBLIC MANAGEMENT AS CYBERSPACE THREATS PROLIFERATE

Introduction. This article examines the critical transformation of the information security paradigm within public management, driven by the escalating scale and sophistication of threats in cyberspace. It argues that the traditional approach to information protection is no longer sufficient in the face of modern challenges, particularly for nations like Ukraine that are at the forefront of hybrid warfare. The analysis is grounded in recent statistics on cyber attacks in Ukraine, a conceptual review of information and cybersecurity, and the resulting necessity for a fundamental enhancement of the nation's security posture.

Materials and Methods. The article is based on general scientific methods for the theoretical substantiation of the importance of cybersecurity in Ukraine under martial law conditions. These methods include explanation, generalization, analysis and synthesis. The informational basis for the research comprised reports from the Cyber Incident Response Operational Center of the State Cyber Protection Center of the State Special Communications Service, scientific publications and media.

Analysis of Literary Sources. The problems of security and information protection have been investigated by O.V. Fedorchuk, V.I. Franchuk, I. Zhdanov, O.S. Kyrychenko, T.V. Subina, B.A. Kormych and others. These works primarily explore general theoretical issues related to information security and relevant activities of specific government bodies.

Highlighting previously unsettled parts of the general problem. The authors did not investigate information protection concerns during martial law conditions and modern trends in the world related to mass increased usage of digital instruments. This gap underscores the need for focused research information security and cybersecurity measures and the strategies required to address these unique challenges effectively during the war.

Results. A core part of the analysis is dedicated to the relationship between the concepts of information security and cybersecurity. The author clarifies that while information security is a broader concept focused on protecting data in all its forms (digital and physical) by ensuring its confidentiality, integrity, and availability (the CIA triad), cybersecurity is a specialized subset focused specifically on protecting digital data, networks, and systems from malicious attacks in the digital realm. The article posits that the evolution of threats requires a paradigm shift where cybersecurity is no longer seen as a purely technical sub-function but as a central, strategic component of national and information security.

Discussion. The paper highlights the acute relevance of this topic for Ukraine, presenting statistics that underscore the dramatic increase in cyber attacks since the full-scale invasion. For instance, it notes a significant surge in state-sponsored phishing campaigns, DDoS attacks on government portals and critical infrastructure, and disinformation campaigns aimed at destabilizing society. The analysis points to a multi-fold increase in registered cyber incidents against state entities, demonstrating that cyberspace has become a primary battlefield.

Conclusion. Given this context, the article concludes that there is an urgent necessity for Ukraine to enhance its information security and cybersecurity posture at the state level. This requires a paradigm shift in public management, moving from a reactive, compliance-based model to a proactive, resilience-focused strategy. This includes not only investing in modern technologies but also fundamentally transforming approaches to risk management, developing the competencies of public servants, fostering public-private partnerships, and integrating cybersecurity considerations into all levels of state policy and decision-making. The ultimate goal is to build a state apparatus that is not only protected but also antifragile–capable of withstanding attacks and adapting to the ever-evolving landscape of cyberspace threats.

Key words: institutional support for the national cybersecurity system, national security, information security, information, cybersecurity, cybercrimes, cyberterrorism, hacking attacks.