Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 351.746:004.056
DOI: 10.32447/20784643.33.2026.17

В. І. Ящук, Р. Л. Ткачук, О. І. Полотай, Б. І. Федина, Є. О. Сєдін
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
ORCID: https://orcid.org/0000-0003-2651-4918 – В.І. Ящук
https://orcid.org/0000-0001-9137-1891 – Р.Л. Ткачук
https://orcid.org/0000-0003-1600-2724 – О.І. Полотай
https://orcid.org/0000-0001-9487-2851 – Б.І. Федина
https://orcid.org/0009-0004-9654-0577 – Є. О. Сєдін
valentina.lender@gmail.com

КОНЦЕПТУАЛЬНІ ТА ПРИКЛАДНІ ЗАСАДИ РЕАЛІЗАЦІЇ КОМПЛЕКСНОГО ПІДХОДУ ДО ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У статті досліджуються концептуальні та прикладні засади реалізації комплексного підходу до забезпечення охорони державної таємниці в системі національної безпеки України. Актуальність дослідження зумовлена зростанням ролі інформаційної безпеки в умовах цифровізації суспільства, посиленням кіберзагроз та гібридних впливів, що безпосередньо впливають на стан національної безпеки України. В умовах воєнно-політичної нестабільності та активного використання інформаційно-комунікаційних технологій особливого значення набуває забезпечення надійної охорони державної таємниці як одного з ключових елементів захисту національних інтересів. Водночас існуюча система охорони державної таємниці характеризується низкою проблем, зокрема фрагментарністю підходів, недостатньою інтегрованістю її складових та обмеженою адаптивністю до сучасних викликів.

Метою дослідження є обґрунтування концептуальних і прикладних засад реалізації комплексного підходу до забезпечення охорони державної таємниці в системі національної безпеки України. У межах дослідження поставлено завдання проаналізувати сучасний стан системи охорони державної таємниці, визначити її основні проблеми, а також розробити ефективний механізм інтеграції організаційних, правових, технічних і кадрових компонентів.

Методологічну основу дослідження становлять методи системного та структурно-функціонального аналізу, що дозволили розглянути систему охорони державної таємниці як цілісну багаторівневу структуру; метод моделювання – для побудови механізму реалізації комплексного підходу; порівняльний аналіз – для зіставлення національних і міжнародних практик у сфері інформаційної безпеки; а також методи узагальнення та систематизації – для формування теоретичних висновків.

У результаті дослідження отримано конкретні наукові результати, що мають як теоретичне, так і прикладне значення. Зокрема, розроблено структурно-функціональну модель системи охорони державної таємниці, яка забезпечує інтеграцію правових, організаційних, технічних і кадрових компонентів у єдину систему управління. На основі цієї моделі обґрунтовано багаторівневий механізм реалізації комплексного підходу, що передбачає узгоджену взаємодію суб'єктів на стратегічному, оперативному та тактичному рівнях, а також запропоновано алгоритм його реалізації, який включає етапи ідентифікації загроз, оцінювання ризиків, впровадження заходів захисту та постійного моніторингу їх ефективності.

Наукова новизна дослідження полягає у формуванні інтегрованої моделі забезпечення охорони державної таємниці, яка базується на комплексному підході та враховує сучасні інформаційні й кібернетичні загрози. Удосконалено підходи до організації системи охорони державної таємниці на основі принципів системності, адаптивності та багаторівневого управління, що дозволяє підвищити ефективність захисту інформації та зміцнити національну безпеку України.

Ключові слова: державна таємниця, національна безпека, комплексний підхід, охорона інформації, нормативно-правові механізми, кіберзагрози, інформаційна безпека, кадровий потенціал, алгоритм проектування системи, модель управління, механізм управління.

V. I. Yashchuk, R. L. Tkachuk, O. I. Polotai, B. I. Fedyna, Ye. O. Sedin
Lviv State University of Life Safety, Lviv, Ukraine

CONCEPTUAL AND APPLIED PRINCIPLES OF IMPLEMENTING A COMPREHENSIVE APPROACH TO PROTECTING STATE SECRETS IN THE NATIONAL SECURITY SYSTEM OF UKRAINE

The article examines the conceptual and applied principles of implementing a comprehensive approach to ensuring the protection of state secrets in the national security system of Ukraine. The relevance of the study is driven by the growing role of information security in the context of the digitalization of society, the strengthening of cyber threats, and hybrid influences that directly affect the state of national security of Ukraine. In the context of military-political instability and the active use of information and communication technologies, ensuring reliable protection of state secrets as one of the key elements of protecting national interests is of particular importance. At the same time, the existing system of protecting state secrets is characterized by a number of problems, in particular, the fragmentation of approaches, insufficient integration of its components, and limited adaptability to modern challenges.

The purpose of the study is to substantiate the conceptual and applied principles of implementing a comprehensive approach to ensuring the protection of state secrets in the national security system of Ukraine. The study aims to analyze the current state of the state secret protection system, identify its main problems, and develop an effective mechanism for integrating organizational, legal, technical, and personnel components.

The methodological basis of the study is the methods of systemic and structural-functional analysis, which allowed us to consider the system of state secret protection as a holistic multi-level structure; the modeling method - to build a mechanism for implementing a comprehensive approach; comparative analysis - to compare national and international practices in the field of information security; as well as methods of generalization and systematization - to form theoretical conclusions.

As a result of the study, specific scientific results were obtained that have both theoretical and applied significance. In particular, a structural and functional model of the state secret protection system was developed, which ensures the integration of legal, organizational, technical, and personnel components into a single management system. Based on this model, a multi-level mechanism for implementing a comprehensive approach was substantiated, which involves coordinated interaction of subjects at the strategic, operational, and tactical levels, and an algorithm for its implementation was proposed, which includes the stages of threat identification, risk assessment, implementation of protection measures, and constant monitoring of their effectiveness.

The scientific novelty of the research lies in the formation of an integrated model for ensuring the protection of state secrets, which is based on a comprehensive approach and takes into account modern information and cyber threats. Approaches to the organization of the state secret protection system have been improved based on the principles of systematicity, adaptability, and multi-level management, which allows for increasing the effectiveness of information protection and strengthening the national security of Ukraine.

Keywords: state secret, national security, comprehensive approach, information protection, regulatory and legal mechanisms, cyber threats, information security, human resources, system design algorithm, management model, management mechanism.

Вступ. У сучасних умовах розвитку інформаційного суспільства та стрімкої цифровізації усіх сфер діяльності держави питання захисту інформації, що становить державну таємницю, набуває особливої актуальності. Посилення гібридних загроз, активне використання інформаційних та кібероперацій у міждержавному протистоянні, а також зростання ролі інформаційних технологій у сфері управління державою обумовлюють необхідність підвищення ефективності системи охорони державної таємниці.

В умовах збройної агресії проти України значно зростає ризик витоку відомостей, що становлять державну таємницю, через технічні канали витоку інформації, кіберзлочинну діяльність, інсайдерські загрози та інші фактори. Це вимагає формування сучасної, багаторівневої та інтегрованої системи захисту секретної інформації, здатної ефективно протидіяти новітнім інформаційним і кіберзагрозам.

Водночас існуюча система охорони державної таємниці потребує подальшого вдосконалення, зокрема щодо інтеграції організаційних, правових, технічних і кадрових механізмів забезпечення режиму секретності. Саме тому актуальним є наукове осмислення концептуальних і прикладних засад реалізації комплексного підходу до забезпечення охорони державної таємниці в системі національної безпеки України.

Охорона державної таємниці є однією з ключових складових системи національної безпеки держави, оскільки забезпечує захист інформації, розголошення якої може завдати шкоди обороноздатності, економічному потенціалу, зовнішньополітичним інтересам та іншим життєво важливим сферам

функціонування держави. Ефективне функціонування системи охорони державної таємниці сприяє збереженню стратегічних ресурсів держави, підтриманню стабільності державного управління та зміцненню оборонного потенціалу країни.

У контексті сучасних безпекових викликів система охорони державної таємниці повинна функціонувати як складний багаторівневий механізм, що поєднує нормативно-правове регулювання, організаційні процедури, технічні засоби захисту інформації, а також підготовку кваліфікованих фахівців у сфері інформаційної безпеки. Реалізація комплексного підходу до забезпечення охорони державної таємниці дозволяє підвищити ефективність функціонування системи національної безпеки та забезпечити належний рівень захисту інформаційних ресурсів держави.

Проблематика забезпечення охорони державної таємниці, а також формування ефективної системи захисту інформації, що становить державну таємницю, перебуває у центрі уваги науковців у галузі національної безпеки, інформаційної безпеки та державного управління. Значний внесок у дослідження теоретичних та практичних аспектів функціонування системи захисту інформації зробили такі українські вчені, як Башта І. І., Гуз А. М., Гулак Г. М., Деркаченко Я. А., Дзюба Т. М., Костюк Ю. В., Лисеюк А. М., Пашорін В. І, Свіріна К. С., Супруненко А. М., Шаблиста О. О. та інші [1-6, 10, 11].

У наукових працях зазначених дослідників розглядаються питання нормативно-правового забезпечення захисту інформації, організаційних механізмів функціонування системи охорони державної таємниці, а також розвитку інформаційної та кібербезпеки держави. Водночас аналіз сучасних наукових публікацій свідчить, що значна частина досліджень зосереджена на окремих аспектах захисту інформації або на правових механізмах забезпечення режиму секретності.

Разом з тим питання формування та реалізації комплексного підходу до забезпечення охорони державної таємниці в системі національної безпеки України, який би поєднував організаційні, правові, технологічні та кадрові складові, потребує подальшого наукового осмислення. Це зумовлює необхідність проведення системного дослідження концептуальних і прикладних засад функціонування такої системи.

Метою дослідження є обґрунтування концептуальних та прикладних засад реалізації комплексного підходу до забезпечення охорони державної таємниці в системі національної безпеки України.

Для досягнення поставленої мети визначено та вирішено такі **завдання:**

– проаналізовано теоретичні підходи до визначення сутності та ролі державної таємниці у системі національної безпеки;

– досліджено нормативно-правові та організаційні механізми функціонування системи охорони державної таємниці в Україні;

– визначено основні загрози та проблеми забезпечення захисту секретної інформації в умовах сучасних інформаційних і кіберзагроз;

– обґрунтовано необхідність реалізації комплексного підходу до забезпечення охорони державної таємниці;

– запропоновано напрями вдосконалення системи охорони державної таємниці в системі національної безпеки України.

Об’єктом дослідження є система забезпечення національної безпеки України у сфері захисту інформації. **Предметом** дослідження є концептуальні та прикладні засади реалізації комплексного підходу до забезпечення охорони державної таємниці.

Методи дослідження. У дослідженні використано комплекс загальнонаукових і спеціальних методів, зокрема метод системного аналізу – для дослідження структури системи охорони державної таємниці та визначення взаємозв’язків між її елементами; порівняльний метод – для аналізу національних і міжнародних підходів до забезпечення інформаційної безпеки; метод структурно-функціонального аналізу – для визначення функцій і ролей суб’єктів системи; метод моделювання – для побудови механізму реалізації комплексного підходу та алгоритму його впровадження; експертно-аналітичний метод – для оцінювання актуальних загроз і визначення напрямів удосконалення системи; методи узагальнення та систематизації – для формування висновків і теоретичних положень дослідження.

Наукова новизна дослідження полягає у формуванні цілісної концептуально-прикладної моделі реалізації комплексного підходу до забезпечення охорони державної таємниці в системі національної безпеки України. У роботі вперше обґрунтовано інтеграцію організаційних, правових, технічних і кадрових механізмів у межах єдиної системи управління, орієнтованої на протидію сучасним інформаційним та кіберзагрозам. Удосконалено підходи до побудови механізму управління охороною державної таємниці на основі багаторівневої структури (макро-, мезо-, мікрорівні), що враховує специфіку суб’єктів, інструментів і

управлінських рішень. Набули подальшого розвитку методичні засади оцінювання ефективності системи охорони державної таємниці через впровадження критеріїв кіберстійкості, адаптивності та інтегрованості системи захисту.

Результати досліджень. Забезпечення охорони державної таємниці є важливою складовою системи національної безпеки держави, оскільки передбачає захист інформації, розголошення якої може завдати шкоди життєво важливим інтересам держави, суспільства та громадян. В умовах сучасного інформаційного суспільства значення ефективної системи захисту державної таємниці суттєво зростає, оскільки інформаційні ресурси стають одним із ключових стратегічних активів держави.

Державна таємниця відповідно до Закону України «Про державну таємницю» визначається як вид інформації з обмеженим доступом, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національним інтересам держави [16]. У контексті реалізації державної політики безпеки, зокрема відповідно до Стратегії національної безпеки України, захист державної таємниці є складовою забезпечення національної безпеки та одним із ключових пріоритетів держави [18]. Водночас Стратегія кібербезпеки України (2021–2025 роки) визначає необхідність посилення заходів із захисту інформації з обмеженим доступом, у тому числі державної таємниці, в інформаційно-комунікаційних системах, що функціонують у кіберпросторі [17]. Відповідно, система охорони державної таємниці являє собою сукупність організаційних, правових, технічних та режимних заходів, спрямованих на запобігання несанкціонованому доступу до секретної інформації, її витоку, втраті або незаконному поширенню [16-18].

Функціонування системи охорони державної таємниці базується на низці принципів, серед яких ключовими є законність, обґрунтованість віднесення інформації до державної таємниці, збалансованість інтересів держави та суспільства, відповідальність за порушення режиму секретності, а також комплексність застосування організаційних, правових і технічних засобів захисту інформації. Реалізація цих принципів забезпечує ефективність функціонування механізмів захисту секретної інформації та сприяє підтриманню належного рівня інформаційної безпеки держави.

Важливою складовою системи охорони державної таємниці є нормативно-правове регулювання, яке визначає порядок віднесення інформації до державної таємниці, встановлює правила поводження з секретною інформацією, регламентує процедури надання доступу до неї, а також визначає відповідальність за порушення режиму секретності. Нормативно-правова база формує основу для організації діяльності органів державної влади, підприємств, установ і організацій, що здійснюють роботу з інформацією, яка становить державну таємницю [12-18].

У сучасних умовах розвитку інформаційно-комунікаційних технологій система охорони державної таємниці повинна враховувати новітні виклики, пов’язані з кіберзагрозами, технічними каналами витоку інформації, а також можливостями несанкціонованого доступу до інформаційних ресурсів через цифрові середовища. Це обумовлює необхідність інтеграції традиційних режимно-секретних заходів із сучасними методами інформаційного та кіберзахисту.

Таким чином, система охорони державної таємниці повинна функціонувати як комплексний багаторівневий механізм, що поєднує нормативно-правове забезпечення, організаційні процедури, технічні засоби захисту інформації та підготовку кваліфікованих фахівців. Реалізація такого підходу дозволяє підвищити ефективність захисту секретної інформації та забезпечити належний рівень інформаційної складової національної безпеки держави.

Функціонування системи охорони державної таємниці в Україні базується на комплексі нормативно-правових актів, що регламентують порядок віднесення інформації до державної таємниці, правила її обробки, зберігання, передачі та використання, а також визначають відповідальність за порушення режиму секретності. Основним законодавчим актом у цій сфері є Закон України «Про державну таємницю», який визначає правові, організаційні та режимні засади охорони секретної інформації, а також порядок її захисту [16]. Водночас Закон України «Про основні засади забезпечення кібербезпеки України» встановлює загальні принципи державної політики у сфері кібербезпеки та визначає необхідність захисту інформації з обмеженим доступом, у тому числі державної таємниці, в інформаційно-комунікаційних системах [12].

Закон встановлює категорії секретності відомостей (державна таємниця, службова таємниця), порядок їх віднесення до певного рівня секретності, вимоги до осіб, які мають доступ до таємної інформації, а також процедури контролю і перевірки дотримання режиму

секретності. Важливе місце займає регламентування процедур доступу до інформації через видачу спеціальних допусків, що забезпечує юридичну та організаційну основу для захисту державної таємниці.

Система контролю доступу до секретної інформації в Україні має комплексний характер і включає як центральні державні органи безпеки, так і внутрішні структурні підрозділи установ, що забезпечують практичну реалізацію режиму секретності та запобігання несанкціонованому розголошенню державної таємниці [7-9]. Система охорони державної таємниці також інтегрується з іншими компонентами національної безпеки, зокрема: кібербезпекою, захистом критичної інфраструктури, оборонною та економічною безпекою. Це забезпечує комплексний підхід до захисту інформації та створює можливість ефективної взаємодії між державними органами, організаціями та фахівцями у сфері безпеки.

Важливою складовою ефективності системи є інституційні механізми, які включають:

– взаємодію центральних та регіональних органів влади;

– міжвідомчі комісії та робочі групи для координації питань безпеки;

– систему підготовки, атестації та контролю кваліфікації фахівців, які мають доступ до секретної інформації.

Сучасні виклики, зокрема активне використання інформаційних технологій і кіберзагроз, вимагають постійного оновлення нормативно-правової бази та вдосконалення інституційних механізмів. Зокрема, необхідно забезпечити:

– впровадження сучасних технічних засобів захисту інформації;

– підвищення обізнаності та кваліфікації персоналу;

– створення інтегрованих систем контролю і моніторингу доступу до секретної інформації.

Таким чином, нормативно-правові та інституційні механізми формують базис для реалізації комплексного підходу до охорони державної таємниці. Їхня ефективність визначає здатність держави захищати стратегічну інформацію, забезпечувати стабільність державного управління та підвищувати рівень національної безпеки.

Реалізація комплексного підходу до охорони державної таємниці передбачає інтеграцію організаційних, правових, технічних та кадрових механізмів захисту інформації в єдину системно узгоджену структуру, що забезпечує ефективне управління ризиками та протидію актуальним і потенційним загрозам. Такий підхід дозволяє поєднати традиційні режимно-секретні заходи із сучасними методами інформаційного та кіберзахисту, формуючи багаторівневу систему контролю доступу до відомостей, що становлять державну таємницю. Організаційна складова комплексного підходу передбачає формування чіткої ієрархічної структури суб'єктів, відповідальних за забезпечення режиму секретності, впровадження процедур управління доступом до секретної інформації, включаючи механізми надання, обліку та припинення допуску, а також організацію систематичного контролю та аудиту дотримання встановлених вимог. Важливим елементом є забезпечення ефективної міжвідомчої взаємодії, що сприяє цілісності та безперервності функціонування системи охорони державної таємниці.

Правова складова комплексного підходу визначає нормативні засади функціонування системи, зокрема регламентує порядок віднесення інформації до державної таємниці, встановлює режим доступу та обмеження щодо її поширення, а також визначає відповідальність за порушення вимог режиму секретності. Водночас важливим напрямом є гармонізація національної нормативно-правової бази з міжнародними стандартами у сфері інформаційної безпеки, що забезпечує узгодженість підходів до захисту інформації в умовах глобалізації та цифровізації.

Технічна складова є невід'ємним елементом сучасної системи охорони державної таємниці та охоплює застосування криптографічних засобів захисту електронних документів і каналів зв'язку, систем моніторингу та контролю доступу до інформаційних ресурсів, а також програмно-апаратних рішень, спрямованих на запобігання несанкціонованому копіюванню, модифікації чи витоку даних. Особливе значення має впровадження інтегрованих систем безпеки, які забезпечують взаємодію технічних засобів із організаційними процедурами, що підвищує загальну ефективність функціонування системи.

Кадровий аспект реалізації комплексного підходу передбачає формування висококваліфікованого кадрового потенціалу у сфері захисту державної таємниці, включаючи підготовку, перепідготовку та підвищення кваліфікації фахівців, оцінювання їх професійних компетентностей, а також впровадження систематичних навчальних заходів і тренінгів, спрямованих на підвищення обізнаності персоналу щодо сучасних загроз і методів їх нейтралізації. Зниження впливу людського фактора розглядається як один із ключових напрямів підвищення ефективності системи.

Впровадження комплексного підходу забезпечує багаторівневий захист секретної інформації, підвищує стійкість системи охорони

державної таємниці до внутрішніх і зовнішніх загроз, сприяє інтеграції правових, організаційних, технічних і кадрових складових у єдину модель управління ризиками, а також оптимізує процеси контролю, аудиту та моніторингу дотримання режиму секретності. Таким чином, реалізація комплексного підходу створює передумови для підвищення ефективності функціонування системи охорони державної таємниці, забезпечує належний рівень інформаційної безпеки держави та сприяє зміцненню національної безпеки України в цілому.

Незважаючи на наявність сформованої законодавчої та організаційної бази, система охорони державної таємниці в Україні функціонує в умовах значних викликів, які об'єктивно знижують її ефективність та потребують системного переосмислення підходів до її організації. Сучасне середовище характеризується стрімким розвитком інформаційних технологій, що зумовлює появу нових каналів витоку інформації та розширення можливостей для несанкціонованого доступу до відомостей, які становлять державну таємницю. Зокрема, активне використання цифрових платформ, мережевих ресурсів та хмарних сервісів формує додаткові кіберзагрози, що вимагають адекватного рівня технічного та криптографічного захисту. Водночас чинна нормативно-правова база не завжди повною мірою враховує сучасні тенденції цифровізації, що проявляється у необхідності її оновлення та гармонізації з міжнародними стандартами, особливо в частині регулювання обігу цифрових носіїв інформації та забезпечення кіберзахисту.

Окрему групу ризиків становлять інсайдерські загрози, пов'язані з діяльністю осіб, які мають допуск до державної таємниці. Недостатній рівень контролю, моніторингу та підготовки персоналу підвищує ймовірність несанкціонованого розголошення інформації, що актуалізує необхідність удосконалення кадрових та організаційних механізмів безпеки. Важливою проблемою залишається також недостатній рівень інтеграції між правовими, організаційними та технічними складовими системи, що ускладнює формування цілісного механізму захисту та знижує оперативність реагування на загрози. Крім того, обмеженість фінансових ресурсів і кадрового потенціалу, зокрема дефіцит висококваліфікованих фахівців у сфері інформаційної безпеки, стримує впровадження сучасних технологічних рішень та інноваційних підходів до захисту інформації.

Аналіз зазначених проблем свідчить про необхідність реалізації комплексного підходу до забезпечення охорони державної таємниці, який передбачає інтеграцію організаційних, правових, технічних та кадрових складових у межах єдиної системи управління безпекою. У цьому контексті ключовими напрямами вдосконалення є оновлення та розвиток нормативно-правового регулювання з урахуванням сучасних викликів, удосконалення організаційних механізмів забезпечення режиму секретності, активне впровадження сучасних інформаційних і кіберзахисних технологій, а також підвищення ефективності міжвідомчої взаємодії. Реалізація зазначених напрямів сприятиме підвищенню рівня захищеності державної таємниці та зміцненню системи національної безпеки України в цілому.

Розглянемо алгоритм реалізації комплексного підходу до забезпечення охорони державної таємниці в системі національної безпеки України (рис. 1), використовуючи при його формуванні окремі елементи традиційних підходів до побудови систем управління безпекою.

На першому етапі здійснюється діагностика існуючого стану системи охорони державної таємниці, зокрема аналізуються організаційні, правові та технічні аспекти забезпечення режиму секретності, а також рівень відповідності встановленим вимогам. Далі проводиться оцінювання необхідності вдосконалення або побудови системи (у разі її недостатньої ефективності або відсутності), що включає: усвідомлення керівництвом сутності, мети та завдань впровадження комплексного підходу; визначення вимог і очікувань зацікавлених сторін (держави, органів влади, установ, персоналу); обґрунтування доцільності розроблення відповідної системи. У разі прийняття рішення про впровадження комплексного підходу формується організаційна структура управління, визначаються відповідальні підрозділи та посадові особи, а також здійснюється розроблення й затвердження плану заходів із забезпечення охорони державної таємниці.

Основні етапи реалізації механізму охоплюють процеси оцінювання ризиків, розроблення та впровадження заходів захисту, організацію режиму секретності, впровадження технічного та криптографічного захисту, а також моніторинг і контроль функціонування системи. Після завершення основних етапів здійснюється оцінювання ефективності функціонування системи, що включає тестування її спроможності протидіяти загрозам, перевірку дотримання вимог режиму секретності та аналіз результатів її функціонування.

У разі позитивного результату на завершальному етапі здійснюється впровадження

та експлуатація системи, що передбачає: моніторинг реалізації заходів; визначення критеріїв оцінювання ефективності; проведення внутрішнього аудиту; розроблення та реалізацію коригувальних заходів. У разі виявлення недоліків або невідповідності встановленим вимогам здійснюється повторне проходження окремих етапів алгоритму, з подальшим повторним оцінюванням системи, що забезпечує її безперервне вдосконалення та адаптацію до сучасних загроз.

Рисунок 1 – Алгоритм проектування системи управління охороною державної таємниці *(розроблено авторами)*

Модель системи реалізації комплексного підходу до забезпечення охорони державної таємниці в системі національної безпеки України представлена на рис. 2. Блок «Цілі системи»: до основних цілей системи належать забезпечення належного рівня захищеності відомостей, що становлять державну таємницю, запобігання їх несанкціонованому розголошенню, витоку чи втраті, а також підвищення рівня кіберстійкості держави. Реалізація зазначених цілей здійснюється через формування та впровадження комплексних програм забезпечення режиму

секретності, які доцільно представляти у вигляді цільових програм у сфері інформаційної безпеки. Такі програми характеризуються сукупністю організаційних, правових, технічних, криптографічних, кадрових та ресурсних показників. Запропонована модель передбачає використання програмно-цільового методу, побудованого за логічною схемою «цілі – завдання – функції – засоби». Спочатку визначаються цілі функціонування системи, далі – завдання їх досягнення, після чого деталізуються функції та відповідні засоби реалізації.

Блок «Функції системи» включає сукупність процесів, спрямованих на забезпечення охорони державної таємниці. Зокрема, функція аналізу середовища передбачає ідентифікацію загроз, формування баз даних інцидентів і класифікацію факторів впливу. Функція моніторингу забезпечує постійне спостереження за станом захищеності інформації, тоді як функція оцінювання ризиків дозволяє визначати рівень небезпеки потенційних загроз. Функція прогнозування реалізується через розроблення сценаріїв розвитку загроз та використання аналітичних і математичних моделей. На основі отриманих результатів здійснюється планування заходів захисту, їх реалізація, контроль виконання та коригування відповідно до змін у середовищі безпеки.

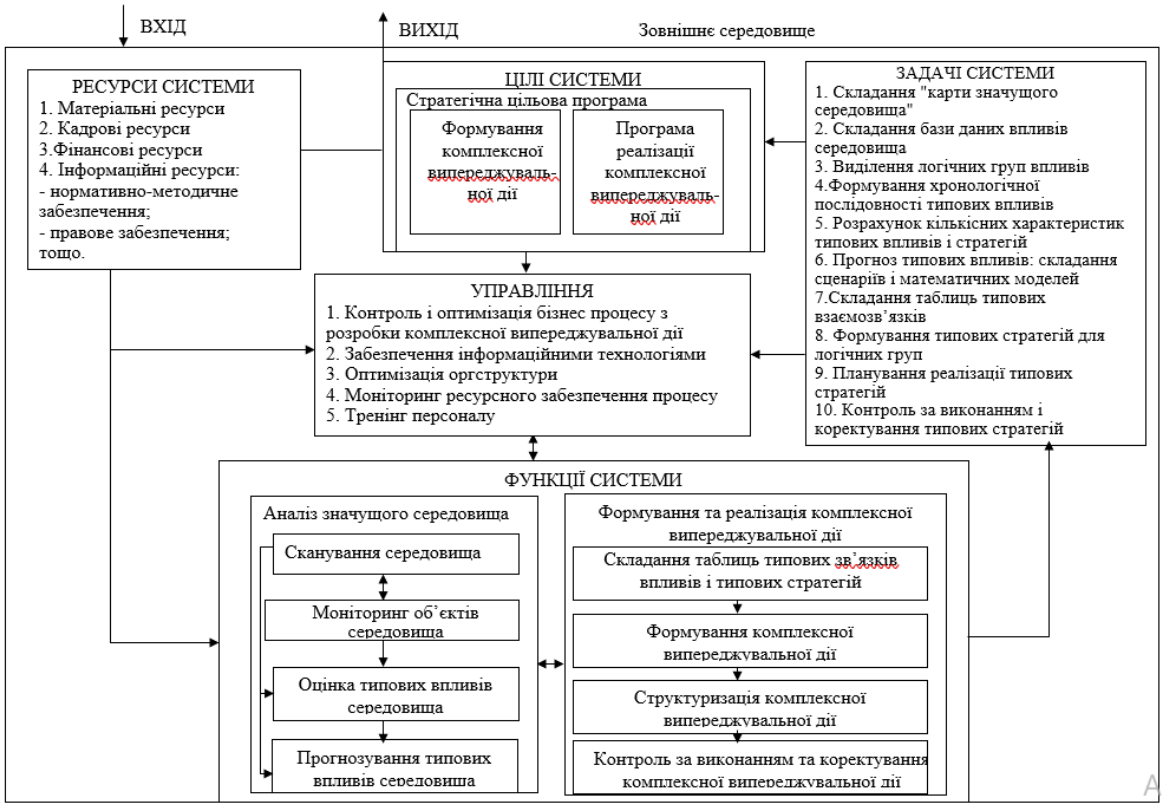

Рисунок 2 – Модель системи управління охороною державної таємниці
(розроблено авторами)

У структурі ресурсного забезпечення системи ключову роль відіграють нормативно-методичне та кадрове забезпечення. Зростають вимоги до кваліфікації фахівців у сфері кібербезпеки та захисту інформації, а також до якості нормативно-методичних матеріалів, що регламентують процеси охорони державної таємниці. Матеріально-технічні ресурси включають засоби технічного і криптографічного захисту інформації, інформаційно-комунікаційну інфраструктуру та програмні засоби моніторингу. Якість ресурсного забезпечення безпосередньо впливає на ефективність функціонування системи та її стійкість до загроз. Прогнозування потреб у ресурсах може здійснюватися із застосуванням нормативного або аналітичного підходів залежно від умов функціонування системи.

Блок «Управління» визначає цілі та завдання функціонування системи у вигляді планових показників забезпечення охорони державної таємниці. На вхід цього блоку надходить інформація про стан зовнішнього і внутрішнього безпекового середовища, наявні ресурси, а також результати функціонування системи. Основним завданням управління є підтримання належного рівня захищеності інформації або його підвищення шляхом прийняття управлінських рішень. У разі виявлення відхилень від

встановлених вимог формується управлінський вплив, спрямований на їх усунення. Таким чином, блок управління охоплює оптимізацію організаційної структури, впровадження інформаційних технологій, контроль і вдосконалення процесів забезпечення режиму секретності, а також моніторинг ресурсного забезпечення.

Запропонована модель системи реалізації комплексного підходу до забезпечення охорони державної таємниці базується на принципах системності, адаптивності та безперервного вдосконалення. Вона інтегрує цілі, функції, завдання, управлінські впливи та ресурсне забезпечення, а її ефективність визначається рівнем досягнення критеріїв захищеності інформації, стійкості до загроз та відповідності вимогам національних та міжнародних стандартів у сфері інформаційної безпеки.

Механізм реалізації комплексного підходу до забезпечення охорони державної таємниці в системі національної безпеки України представлений на рисунку 3 і втілює ключові ідеї дослідження:

– механізм забезпечення охорони державної таємниці є багаторівневим і функціонує на макро-, мезо- і мікрорівнях, при цьому суб'єкти, управлінські рішення та інструменти на кожному рівні мають специфічні особливості, зумовлені характером загроз і функціональним призначенням відповідних структур;

– механізм спрямований на узгодження інтересів основних суб'єктів системи національної безпеки: держави – щодо збереження критично важливої інформації; органів сектору безпеки і оборони – щодо забезпечення стійкості управління; суб'єктів господарювання – щодо захисту інформаційних активів; суспільства – щодо гарантування безпеки та стабільності;

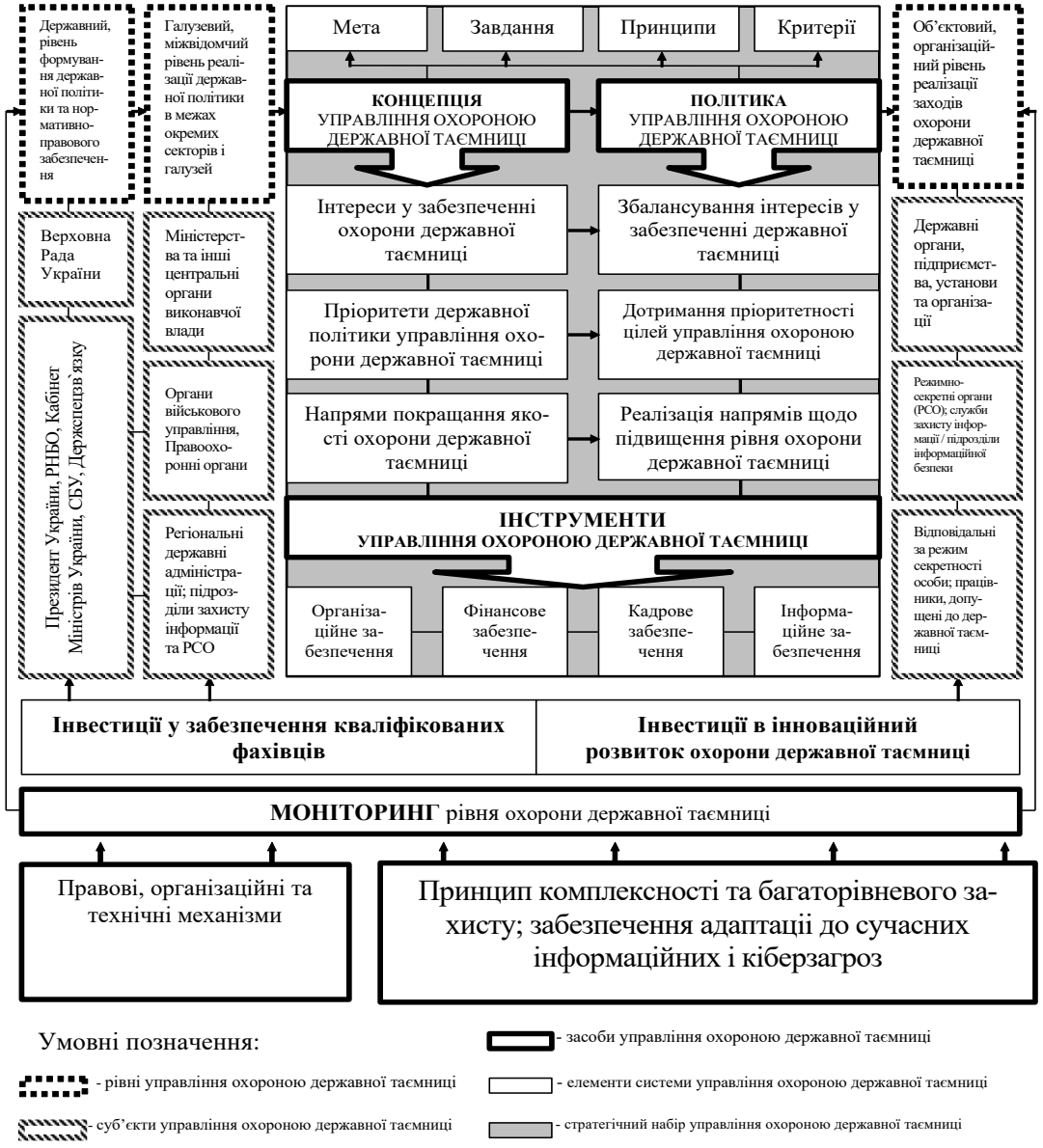

Рисунок 3 – Механізм управління системою охорони державної таємниці
(розроблено авторами)

– забезпечення охорони державної таємниці здійснюється через поєднання державного та відомчого регулювання, де законодавчі та нормативно-правові акти встановлюють обов'язкові вимоги до режиму секретності, а відомчі та локальні документи конкретизують механізми їх реалізації з урахуванням специфіки діяльності;

– в основу механізму покладено принцип відповідності рівня захищеності інформації актуальним загрозам, що передбачає адаптацію системи охорони державної таємниці до динаміки кіберзагроз, гібридних впливів та розвитку інформаційних технологій; при цьому рівень захисту має відповідати значущості інформації та потенційним наслідкам її розголошення;

– об'єктом управлінського впливу є процеси створення, обробки, передачі, зберігання та знищення відомостей, що становлять державну таємницю, а також інфраструктура, що забезпечує їх функціонування;

– на організаційному (об'єктовому) рівні управління охороною державної таємниці здійснюється через розроблення та впровадження комплексних програм забезпечення режиму секретності, які включають етапи оцінювання ризиків, планування заходів захисту, їх реалізацію, контроль та вдосконалення; алгоритм реалізації таких програм визначає послідовність управлінських дій у системі забезпечення безпеки;

– реалізується механізм забезпечення охорони державної таємниці через досягнення встановлених критеріїв ефективності, зокрема: забезпечення конфіденційності, цілісності та доступності інформації, контрольованість доступу, стійкість до кіберзагроз, своєчасність виявлення та реагування на інциденти, а також відповідність національним і міжнародним стандартам у сфері інформаційної безпеки.

Вдосконалення системи охорони державної таємниці має ґрунтуватися на інтеграції концептуальних і прикладних підходів, що забезпечує формування цілісної, адаптивної та ефективної моделі захисту інформації в умовах сучасних безпекових викликів. Одним із ключових напрямів є модернізація нормативно-правової бази, яка передбачає оновлення законодавства з урахуванням розвитку інформаційних технологій, актуалізації кіберзагроз та необхідності гармонізації з міжнародними стандартами у сфері інформаційної безпеки. Особливої уваги потребує вдосконалення процедур присвоєння допусків до державної таємниці, механізмів контролю доступу, а також підвищення ефективності системи відповідальності за порушення режиму секретності.

Важливим аспектом є підвищення ефективності організаційних механізмів, що передбачає оптимізацію структури органів, відповідальних за забезпечення охорони державної таємниці, впровадження системного підходу до моніторингу та аудиту дотримання режиму секретності, а також посилення міжвідомчої взаємодії з метою забезпечення узгодженості дій усіх суб'єктів системи. Паралельно необхідним є активне впровадження сучасних технічних засобів захисту, зокрема застосування криптографічних і програмно-апаратних рішень для захисту електронної інформації, створення інтегрованих систем контролю та моніторингу витоку даних, а також забезпечення безпечного зберігання і передачі інформації на цифрових носіях.

Суттєвого значення набуває розвиток кадрового потенціалу, що передбачає організацію систематичного навчання та підвищення кваліфікації персоналу, який працює з відомостями, що становлять державну таємницю, формування компетентностей у сфері протидії сучасним кіберзагрозам, а також удосконалення системи оцінювання та контролю знань працівників, допущених до секретної інформації. Не менш важливим є забезпечення інтеграції системи охорони державної таємниці з національною системою кібербезпеки, що передбачає поєднання організаційних, правових і технічних засобів захисту з заходами кіберзахисту, використання аналітичних та моніторингових інструментів для виявлення загроз у режимі реального часу, а також налагодження ефективної взаємодії між державними органами, суб'єктами господарювання та закладами освіти з метою підготовки висококваліфікованих фахівців. Реалізація зазначених напрямів забезпечує формування стійкої, інтегрованої та ефективної системи охорони державної таємниці, здатної адекватно реагувати на сучасні загрози, гарантувати належний рівень захисту інформації та сприяти зміцненню національної безпеки України.

Висновки. Результати дослідження підтверджують, що ефективне функціонування системи охорони державної таємниці є ключовим елементом забезпечення національної безпеки України. Теоретичний аналіз дозволив уточнити сутність державної таємниці як інформації, розголошення якої завдає шкоди життєво важливим інтересам держави, та обґрунтувати необхідність її захисту на основі комплексного поєднання правових, організаційних, технічних і кадрових компонентів.

На відміну від узагальнених підходів, у роботі розроблено структурно-функціональну модель системи охорони державної таємниці, яка інтегрує зазначені компоненти в єдину керовану систему з урахуванням сучасних кіберзагроз і цифровізації інформаційних процесів. Запропонована модель передбачає взаємодію суб'єктів на стратегічному, оперативному та тактичному рівнях і забезпечує узгодженість управлінських рішень.

Крім того, обґрунтовано багаторівневий механізм реалізації комплексного підходу, який

включає: нормативно-правовий рівень (оновлення законодавства та гармонізація з кібербезпековими стандартами); організаційний рівень (оптимізація структури управління та розподілу повноважень); технічний рівень (впровадження сучасних засобів захисту інформації); кадровий рівень (підготовка та підвищення кваліфікації персоналу).

Важливим науковим результатом є також розроблення алгоритму реалізації комплексного підходу до охорони державної таємниці, який передбачає послідовність етапів: ідентифікацію загроз, оцінювання ризиків, вибір і впровадження заходів захисту, моніторинг ефективності та адаптацію системи до змінного кіберсередовища. Запропонований алгоритм орієнтований на ризик-менеджмент і забезпечує адаптивність системи до гібридних загроз.

Встановлено, що основними проблемами функціонування системи залишаються недостатня інтеграція складових, обмежені ресурси, людський фактор та зростання інтенсивності кіберзагроз. Доведено, що їх подолання можливе саме через впровадження запропонованих моделі, механізму та алгоритму, які формують цілісну методологічну основу модернізації системи.

Таким чином, у роботі не лише узагальнено теоретичні положення, а й отримано конкретні наукові результати, що полягають у розробленні та обґрунтуванні моделі, механізму й алгоритму реалізації комплексного підходу до охорони державної таємниці. Їх практичне впровадження сприятиме підвищенню ефективності захисту секретної інформації, зміцненню національної безпеки та підвищенню стійкості державних інституцій до сучасних інформаційних і кіберзагроз.

Перспективи подальших досліджень пов’язані з розробленням методів кількісного оцінювання ефективності запропонованої моделі, удосконаленням ризик-орієнтованих підходів в умовах гібридних загроз, а також інтеграцією національної системи захисту з міжнародними стандартами кібербезпеки та використанням технологій штучного інтелекту для автоматизації процесів моніторингу й прогнозування загроз.

Список літератури:

1. Супруненко А. М., Башта І. І., Лисеюк А. М., Свіріна К. С. Організація охорони державної таємниці в Україні : навч. посіб. Ірпінь : УДФСУ, 2020. 370 с.
2. Шаблиста О. О. Кримінально-правова охорона відомостей, що становлять державну та службову таємницю Національної поліції України : дис. ... д-ра філос. : 081 / Дніпров. держ. ун-т внутр. справ. Дніпро, 2025.
3. Охорона державної таємниці в Україні : навч. посіб. / А. М. Гуз та ін. Київ : Нац. акад. СБУ, 2017. 216 с.
4. Безпека інформаційно-комунікаційних систем : підручник / Ю. В. Костюк та ін. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 1016 с.
5. Системи захисту інформації : підручник / Ю. В. Костюк та ін. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 887 с.
6. Пашорін В. І., Костюк Ю. В. Безпека інформаційних систем : навч. посіб. Київ : Держ. торг.-екон. ун-т, 2023. 376 с.
7. Ящук В. І. Організація багаторівневої системи охорони державної таємниці в умовах воєнного стану. *Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану* : тези ІІІ Міжнар. наук.-практ. конф. (Хмельницький, 21 листоп. 2024 р.). Хмельницький : Вид-во НАДПСУ, 2025. С. 1226–1229.
8. Ящук В., Ошурко Б. Сучасні виклики захисту державної таємниці в умовах війни. *Інформаційна безпека та інформаційні технології* : зб. доповідей V Міжнар. наук.-практ. конф. (ІБІТ 2024, м. Львів, 27 листоп. 2024 р.). Львів : ЛДУ БЖД, 2024. С. 17–20.
9. Yashchuk V., Demyanchuk Y., Savitska V. Integrative approach to the analysis, modeling, and ensuring cyber security of critical information infrastructure under modern threats. *Baltic Journal of Economic Studies*. 2025. Vol. 11, No. 2. P. 273–286. DOI: https://doi.org/10.30525/2256-0742/2025-11-2-273-286.
10. Інформаційна та кібернетична безпека підприємства : підручник / Г. М. Гулак та ін. Львів : Видавець Марченко Т. В., 2023. 370 с.
11. Деркаченко Я. А., Дзюба Т. М. Забезпечення кіберстійкості України за сучасних умов: цифрові навички та компетентності. *Зв'язок,* 2021. № 3. С. 12 – 17. DOI: 10.31673/2412-9070.2021.031216.
12. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII (ред. від 24.10.2020). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
13. Про криптографічний та технічний захист інформації : Закон України від 22.05.2003 № 850-IV. URL: https://ips.ligazakon.net/document/NT1819.
14. Інформаційна та кібербезпека: соціотехнічний аспект / В. Л. Бурячок та ін. URL: http://www.dut.edu.ua/uploads/p_303_79299367.pdf
15. Кібербезпека в інформаційному суспільстві : інформаційно-аналітичний дайджест / відп. ред. О. Довгань. Київ : ДНУ ІІБП НАПрН України ; НБУВ, 2025. № 10 (жовтень). 166 с.
16. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
17. Стратегія кібербезпеки України (2021–2025 роки) : затв. Указом Президента України від 26.08.2021 № 447/2021. URL:

https://www.rnbo.gov.ua/files/2021/Cybersecurity_Strategy.pdf.

18. Стратегія національної безпеки України : затв. Указом Президента України від 14.09.2020 № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037.

References:

1. Suprunenko, A. M., Bashta, I. I., Lysejuk, A. M., & Svirina, K. S. (2020). *Orhanizatsiia okhorony derzhavnoi taiemnytsi v Ukraini* [Organization of state secrets protection in Ukraine]. Irpin: University of the State Fiscal Service of Ukraine. 370 p.

2. Shablysta, O. O. (2025). *Kryminalno-pravova okhorona vidomostei, shcho stanovliat derzhavnu ta sluzhbovu taiemnytsiu Natsionalnoi politsii Ukrainy* [Criminal law protection of state and official secrets of the National Police of Ukraine] (Doctoral dissertation). Dnipro State University of Internal Affairs, Dnipro [in Ukrainian].

3. Huz, A. M., et al. (2017). *Okhorona derzhavnoi taiemnytsi v Ukraini* [Protection of state secrets in Ukraine]. Kyiv: National Academy of the Security Service of Ukraine. 216 p. [in Ukrainian].

4. Kostiuk, Yu. V., et al. (2025). *Bezpeka informatsiino-komunikatsiinykh system* [Security of information and communication systems]. Kyiv: Borys Grinchenko Kyiv Metropolitan University. 1016 p. [in Ukrainian].

5. Kostiuk, Yu. V., et al. (2025). *Systemy zakhystu informatsii* [Information protection systems]. Kyiv: Borys Grinchenko Kyiv Metropolitan University. 887 p. [in Ukrainian].

6. Pashorin, V. I., & Kostiuk, Yu. V. (2023). *Bezpeka informatsiinykh system* [Information systems security]. Kyiv: State University of Trade and Economics. 376 p. [in Ukrainian].

7. Yashchuk, V. I. (2025). Orhanizatsiya bahatorivnevoyi systemy okhorony derzhavnoyi tayemnytsi v umovakh voyennoho stanu [Organization of a multi-level system of state secrets protection under martial law]. In *Security and defense sector of Ukraine in protecting national interests: current problems and tasks under martial law* (pp. 1226–1229). Khmelnytskyi: National Academy of the State Border Guard Service of Ukraine.

8. Yashchuk, V., & Oshurko, B. (2024). Modern challenges of state secrets protection under wartime conditions. In *Proceedings of the V International Scientific and Practical Conference "Information Security and Information Technologies"* (pp. 17–20). Lviv: Lviv State University of Life Safety.

9. Yashchuk, V., Demyanchuk, Y., & Savitska, V. (2025). Suchasni vyklyky zakhystu derzhavnoyi tayemnytsi v umovakh viyny [Integrative approach to the analysis, modeling, and ensuring cybersecurity of critical information infrastructure under modern threats]. *Baltic Journal of Economic Studies, 11*(2), 273–286. https://doi.org/10.30525/2256-0742/2025-11-2-273-286

10. Hulak, H. M., et al. (2023). *Informatsiina ta kibernetychna bezpeka pidpryiemstva* [Information and cyber security of enterprise]. Lviv: Marchenko T. V. 370 p. [in Ukrainian].

11. Derkachenko, Ya. A., & Dziuba, T. M. (2021). Zabezpechennya kiberstiykosti Ukrayiny za suchasnykh umov: tsyfrovi navychky ta kompetentnosti [Ensuring cyber resilience of Ukraine under modern conditions: digital skills and competencies]. *Zviazok*, (3). P. 12–17. https://doi.org/10.31673/2412-9070.2021.031216 [in Ukrainian].

12. Verkhovna Rada of Ukraine. (2017). *On the basic principles of cybersecurity of Ukraine* (Law No. 2163-VIII, as amended 2020). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19

13. Verkhovna Rada of Ukraine. (2003). *On cryptographic and technical protection of information* (Law No. 850-IV). Retrieved from https://ips.ligazakon.net/document/NT1819

14. Buriachok, V. L., et al. (n.d.). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt* [Information and cybersecurity: socio-technical aspect]. Retrieved from http://www.dut.edu.ua/uploads/p_303_79299367.pdf [in Ukrainian].

15. Dovhan, O. (ed.). (2025). *Cybersecurity in the information society: analytical digest*, No. 10. Kyiv: Institute of Information Security and Law of the National Academy of Legal Sciences of Ukraine; Vernadsky National Library of Ukraine. 166 p. [in Ukrainian].

16. Verkhovna Rada of Ukraine. (1994). *On state secrets* (Law No. 3855-XII). Retrieved from https://zakon.rada.gov.ua/laws/show/3855-12 [in Ukrainian].

17. President of Ukraine. (2021). *Cybersecurity Strategy of Ukraine (2021–2025)* (Decree No. 447/2021). Retrieved from https://www.rnbo.gov.ua/files/2021/Cybersecurity_Strategy.pdf [in Ukrainian].

18. President of Ukraine. (2020). *National Security Strategy of Ukraine* (Decree No. 392/2020). Retrieved from

19. https://www.president.gov.ua/documents/3922020-35037 [in Ukrainian].

Науково-методична стаття.
Надійшла до редакції 27.03.2026.
Прийнята до друку 29.04.2026.
Опублікована 25.05.2026.