



EAST EUROPEAN ASSOCIATION OF SCIENTISTS

СУЧАСНІ ВИКЛИКИ ТА СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОЇ БЕЗПЕКИ:

**ЕКОНОМІЧНИЙ, СОЦІАЛЬНИЙ,
ПСИХОЛОГІЧНИЙ,
ІНФОРМАЦІЙНИЙ,
ВІЙСЬКОВИЙ, ПРАВОВИЙ ТА
ОСВІТНІЙ ВИМІРИ**

Колективна монографія

***за редакцією д-ра держ. упр.,
проф. З. М. Бурик***

WARSAW, POLAND 2025

СУЧАСНІ ВИКЛИКИ ТА СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОЇ БЕЗПЕКИ: ЕКОНОМІЧНИЙ, СОЦІАЛЬНИЙ, ПСИХОЛОГІЧНИЙ, ІНФОРМАЦІЙНИЙ, ВІЙСЬКОВИЙ, ПРАВОВИЙ ТА ОСВІТНІЙ ВИМІРИ

КОЛЕКТИВНА МОНОГРАФІЯ

за редакцією д-ра держ. упр., проф. З. М. Бурик



Warsaw, Poland 2025

Автори: Зоряна Бурик (ред.), Андрій Шинькович (розділ 1), Наталія Росоха (розділ 2), Тетяна Ханецька, Світлана Поліщук (розділ 3), Юрій Коміренко (розділ 4), Катерина Якушко (розділ 5), Ольга Гончарук (розділ 6), Ігор Горбань (розділ 7), Валерій Зубенко (розділ 8), Юрій Чикриж (розділ 9), Уляна Безкоровайна, Роксолана Неділько, Оксана Яремчук (розділ 10), Оксана Приходько (розділ 11), Андрій Войцещук, Інна Гуцул, Віктор Мартинюк (розділ 12), Олена Мартиненко (розділ 13), Юрій Бондаренко (розділ 14), Аліна Парасей-Гочер, Інна Цибенко (розділ 15), Катерина Гурковська (розділ 16), Олександра Кузьменко, Альона Пашенко (розділ 17), Микола Старинський, Жанна Завальна (розділ 18).

Рецензенти **О. І. Пархоменко-Куцевіл**, д-р держ. упр., професор, Університет Григорія Сковороди в Переяславі.
 О. В. Птащенко, д-р екон. наук, професор, Західноукраїнський національний університет.
 Г. М. Сjuta, д-р філол. наук, професор, Інститут української мови Національної академії наук України.

Рекомендовано до публікації рішенням науково-технічної радиГО «Східно-Європейська спілка науковців» (протокол № 19 від 27 жовтня 2025 року).

С 93 Сучасні виклики і стратегії забезпечення комплексної безпеки: економічний, соціальний, психологічний, інформаційний, військовий, правовий та освітній виміри = Contemporary Challenges and Strategies for Ensuring Comprehensive Security: Economic, Social, Psychological, Information, Military, Legal, and Educational Dimensions : колективна монографія ; за редакцією д-ра держ. упр., проф. З. М. Бурик. — Warsaw : East European Association of Scientists, 2025. — viii+481 p. DOI: <http://doi.org/10.5281/zenodo.17636317>

ISBN 978-83-68212-07-5 (e-Book)

Монографія присвячена комплексному дослідженню сучасних викликів та стратегій забезпечення комплексної безпеки держави і суспільства. У роботі розглянуто ключові виміри безпеки, зокрема економічний, соціальний, психологічний, правовий та інформаційний. Проведено аналіз загроз, що виникають в умовах воєнного стану та глобальних трансформацій. Окрему увагу приділено проблемам соціально-психологічної адаптації населення, зокрема з посттравматичним синдромом в учасників бойових дій, емоційною вразливістю підлітків, роботою на деокупованих територіях та вдосконаленню правових механізмів захисту прав військовослужбовців, корпоративних прав, протидії тероризму та домашньому насильству. Запропоновано стратегічні підходи до посилення стійкості держави, що враховують як управлінські інновації, так і роль громадянського суспільства.

УДК 351.86:355/359:338.2:004.9:316.4

ISBN 978-83-68212-07-5 (e-Book)

© Авторів окремих розділів, 2025

UDK 351.86:355/359:338.2:004.9:316.4

Authors:

Edited by **Zoriana Buryk**

Andrii Shynkovych (Chapter 1), **Nataliia Rosokha** (Chapter 2), **Tetiana Khanetska**, **Svitlana Polishchuk** (Chapter 3), **Yurii Komirenko** (Chapter 4), **Kateryna Yakushko** (Chapter 5), **Olha Honcharuk** (Chapter 6), **Ihor Horban** (Chapter 7), **Valerii Zubenko** (Chapter 8), **Yurii Chykryzh** (Chapter 9), **Uliana Bezkorovaina**, **Roksolana Nedilko**, **Oksana Yaremchuk** (Chapter 10), **Oksana Prykhodko** (Chapter 11), **Andrii Voitseshchuk**, **Inna Hutsul**, **Viktor Martyniuk** (Chapter 12), **Olena Martynenko** (Chapter 13), **Yurii Bondarenko** (Chapter 14), **Alina Parasiei-Hocher**, **Inna Tsybenko** (Chapter 15), **Kateryna Hurkovska** (Chapter 16), **Oleksandra Kuzmenko**, **Alona Pashchenko** (Chapter 17), **Mykola Starynskyi**, **Zhanna Zavalna** (Chapter 18).

Z. Buryk (Ed.), *Contemporary Challenges and Strategies for Ensuring Comprehensive Security: Economic, Social, Psychological, Information, Military, Legal, and Educational Dimensions*: collective monograph. Warsaw: East European Association of Scientists, 2025. viii+481 p.
<http://doi.org/10.5281/zenodo.17636317>

Reviewers:

Oksana Parkhomenko-Kutsevil, *Doctor of Sciences (Public Administration), Professor, Hryhorii Skovoroda University in Pereiaslav.*

Olena Ptaschenko, *Doctor of Sciences (Economics), Professor, West Ukrainian National University.*

Halyna Siuta, *Doctor of Sciences (Philology), Professor, Institute of the Ukrainian Language of the National Academy of Sciences of Ukraine.*

ISBN 978-83-68212-07-5 (eBook)

East European Association of Scientists *sp. z o. o.*
ul. JANOWIECKA, nr 17A, lok. 3, miejsc. WARSZAWA,
kod 03-887, poczta WARSZAWA, kraj POLSKA
Copyright © 2025 Authors. All rights reserved.



The e-book is published at  <https://www.eeast.net>



This Open Access e-book is licensed under a Creative Commons Attribution-NonCommercial (CC BY-NC) 4.0 International License.

No part of this e-book may be reproduced, transmitted, or converted in any format or by any electronic, mechanical, recording, or other means without the written permission of the Eastern European Association of Scientists *sp. z o. o.*

The author is solely responsible for the accuracy of the translation, facts, quotations, place names, proper names, organizations, companies, institutions, and other data.

Publisher: Myroslav Buryk

Editorial Project Manager: Zoriana Buryk

Production Project Manager: Mykola Biloshkurskyi

ЗМІСТ

РОЗДІЛ 1. Інформаційно-аналітичне забезпечення асекурації продовольчої безпеки: методологія, індикатори та напрями удосконалення.....	1
РОЗДІЛ 2. Вплив цифрових трансформацій на соціальну стабільність: забезпечення соціальної безпеки та інклюзії методами соціальної роботи.....	35
РОЗДІЛ 3. Стратегії подолання ПТСР в учасників бойових дій.....	70
РОЗДІЛ 4. Національні культури – гарант збереження людської ідентичності, духовного виміру людства та миру в умовах глобальних викликів.....	104
РОЗДІЛ 5. Cultural Safety: Dialogue, Tolerance, Conflict Prevention.....	150
РОЗДІЛ 6. Боротьба з тероризмом через призму правового регулювання.....	187
РОЗДІЛ 7. Роль технологічних аспектів у вирощуванні сої як чинника продовольчої безпеки України.....	205
РОЗДІЛ 8. Підвищення ефективності вирощування кукурудзи на зерно через оптимізацію технології для забезпечення продовольчих потреб України.....	222
РОЗДІЛ 9. Вплив елементів технології вирощування на продуктивність гороху в контексті продовольчої стабільності України.....	239
РОЗДІЛ 10. Державне управління у сфері охорони здоров'я в контексті комплексної безпеки: виклики та стратегічні підходи.....	256
РОЗДІЛ 11. Правові виклики та механізми захисту прав військовослужбовців як елемент забезпечення комплексної безпеки в умовах збройних конфліктів.....	272

РОЗДІЛ 12. Правовий механізм захисту корпоративних прав у системі забезпечення національної безпеки.....	305
РОЗДІЛ 13. Соціальна робота в умовах деокупації: виклики, стратегії, роль благодійних фондів.....	337
РОЗДІЛ 14. Фандрейзинг у діяльності благодійних фондів: сучасні підходи та безпековий вимір.....	366
РОЗДІЛ 15. Емоційна вразливість підлітків у воєнний час як фактор соціально-психологічної безпеки: виклики, прояви, напрями підтримки.....	399
РОЗДІЛ 16. Основні проблеми та шляхи вдосконалення діяльності суб'єктів, що здійснюють заходи у сфері запобігання та протидії домашньому насильству в умовах воєнного стану.....	415
РОЗДІЛ 17. Прогнозування розвитку торговельного підприємства: практичне застосування сценарного підходу та моделей штучного інтелекту.....	434
РОЗДІЛ 18. Бюро економічної безпеки в механізмі забезпечення фінансової безпеки держави та її сталого розвитку.....	462

АНОТАЦІЯ

Колективна монографія присвячена комплексному дослідженню сучасних викликів та стратегій забезпечення комплексної безпеки України. Актуальність роботи зумовлена безпрецедентними загрозами, що постали перед державою та суспільством внаслідок повномасштабної збройної агресії, глобальних трансформацій та необхідності адаптації системи державного управління до умов воєнного стану. Традиційні підходи до безпеки виявляються недостатніми, що вимагає міждисциплінарного аналізу її ключових вимірів: економічного, соціального, психологічного, інформаційного, військового, правового та освітнього. Метою монографії є теоретико-методологічне обґрунтування та розробка практичних стратегій для посилення стійкості держави. Це включає аналіз специфічних загроз у кожному з вимірів безпеки та формування інноваційних управлінських підходів, спрямованих на захист населення, збереження ідентичності та забезпечення сталого розвитку в умовах екзистенційних викликів.

У монографії детально проаналізовано багатовимірну структуру комплексної безпеки. В економічному вимірі особливу увагу приділено забезпеченню продовольчої безпеки. Досліджено інформаційно-аналітичні підходи до її асекурації та проаналізовано конкретні технологічні аспекти вирощування стратегічних культур (сої, кукурудзи та гороху) для задоволення продовольчих потреб. Окремо розглянуто механізми забезпечення фінансової безпеки держави, зокрема роль Бюро економічної безпеки, та застосування сучасних методів прогнозування, включаючи сценарний підхід та моделі штучного інтелекту, для управління розвитком підприємств.

Глибоко досліджено соціально-психологічний вимір, що опинився під найбільшим тиском внаслідок війни. Запропоновано конкретні стратегії подолання посттравматичного стресового розладу в учасників бойових дій. Проаналізовано виклики соціально-психологічної адаптації населення, зокрема емоційну вразливість підлітків у воєнний час. Розглянуто нові завдання соціальної роботи в умовах цифрових трансформацій та специфіку її організації на деокупованих територіях, підкреслюючи роль благодійних фондів та фандрейзингу в цьому процесі. Також проаналізовано проблеми протидії домашньому насильству в умовах воєнного стану.

У правовому та адміністративному вимірі робота фокусується на адаптації законодавства до нових загроз. Проаналізовано правове регулювання боротьби з тероризмом, механізми захисту прав військовослужбовців та захисту корпоративних прав як елементу національної безпеки. Окремий розділ присвячено викликам та стратегічним підходам у державному управлінні сферою охорони здоров'я в контексті комплексної безпеки.

Нарешті, у культурному та інформаційному вимірі обґрунтовано роль національних культур як гаранта збереження ідентичності та проаналізовано концепцію «культурна безпека» (cultural safety), діалогу та толерантності як інструментів запобігання конфліктам.

Дослідження підтверджує, що забезпечення комплексної безпеки в сучасних умовах вимагає системного та інтегрованого підходу, що виходить за межі суто військової чи економічної сфери. Монографія доводить, що стійкість держави (state resilience) ґрунтується на синергії ефективного державного управління, стійкої соціально-психологічної адаптації суспільства, надійних правових механізмів та збереженні культурної ідентичності.

Автори наголошують на необхідності впровадження інноваційних управлінських моделей, активної цифрової трансформації соціальної сфери та посилення взаємодії між державними інституціями та громадянським суспільством, зокрема благодійними фондами. Запропоновані у роботі стратегії та практичні рекомендації спрямовані на посилення здатності України протистояти гібридним загрозам та забезпечити основу для сталого повоєнного відновлення.

КЛЮЧОВІ СЛОВА:

продовольча безпека, соціальна безпека, посттравматичний стресовий розлад (ПТСР), націоналізм, культурна безпека (cultural safety), тероризм, соя, кукурудза, горох, державне управління, військовослужбовці, корпоративні права, соціальна робота, фандрейзинг, підлітки, домашнє насильство, прогнозування, фінансова безпека.

РОЗДІЛ 10.

ДЕРЖАВНЕ УПРАВЛІННЯ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я В КОНТЕКСТІ КОМПЛЕКСНОЇ БЕЗПЕКИ: ВИКЛИКИ ТА СТРАТЕГІЧНІ ПІДХОДИ

<http://doi.org/10.5281/zenodo.17639867>

УЛЯНА БЕЗКОРОВАЙНА

КЗВО ЛОР «Львівська медична академія імені Андрея Крупинського».

Доцент кафедри внутрішньої медицини та управління охороною здоров'я,
к. держ. упр., доцент.

РОКСОЛАНА НЕДІЛЬКО

КЗВО ЛОР «Львівська медична академія імені Андрея Крупинського».

Доцент кафедри внутрішньої медицини та управління охороною здоров'я,
к. держ. упр., доцент.

ОКСАНА ЯРЕМЧУК

КЗВО ЛОР «Львівська медична академія імені Андрея Крупинського».

Асистент кафедри внутрішньої медицини та управління охороною здоров'я,
к. держ. упр.

E-mail: akantlvov1@ukr.net

У сучасному світі система охорони здоров'я виступає не лише як інструмент медичного обслуговування населення, але й як ключовий елемент національної безпеки. Стрімке зростання кількості транснаціональних ризиків – пандемій, екологічних катастроф, кіберзагроз, соціальних потрясінь та військових конфліктів – вимагає переосмислення механізмів державного управління в медичній сфері з позицій комплексної безпеки.

Особливу актуальність дослідження набуває в умовах тривалої безпекової кризи, спричиненої російською агресією проти України. Медична інфраструктура країни зазнає системних викликів, що вимагає оперативного, ефективного та стратегічно виваженого управлінського реагування. При цьому охорона здоров'я повинна функціонувати не лише як «реактивна система», а як ресурс стійкості держави – здатна адаптуватись, забезпечувати життєво необхідні послуги та захищати здоров'я громадян в умовах невизначеності.

Концепт комплексної безпеки передбачає інтеграцію медичних, соціальних, екологічних, інформаційних і технологічних компонентів у систему стратегічного управління. Це відкриває нові можливості для побудови інноваційних моделей державного управління, що базуються на міжвідомчій координації, цифровій трансформації, стійкості до криз та партнерстві з громадянським суспільством і міжнародними інституціями.

У цьому контексті особливого значення набуває формування стратегічних підходів, здатних забезпечити ефективну реакцію держави на комплексні загрози й одночасно сприяти довгостроковому розвитку сфери охорони здоров'я. Розкриття викликів та перспектив у межах такої парадигми є не лише науково обґрунтованим, але й практично необхідним завданням для формування політики безпеки держави.

В умовах зростаючої складності проблем державного управління в охороні здоров'я, зумовленої багатовимірними загрозами безпекового характеру, особливої ваги набуває термінологічна визначеність і концептуальна впорядкованість.

Дослідження проблеми державного управління сферою охорони здоров'я доцільно розпочати з визначення такого складного поняття, як «здоров'я». Існує низка дефініцій, які характеризують це поняття з різних точок зору – соціальної, біологічної, медичної тощо. Серед них найбільш відомим є визначення Статуту Всесвітньої організації охорони здоров'я

(ВООЗ): «Здоров'я є стан повного фізичного, духовного і соціального благополуччя, а не тільки відсутність хвороби або недуги» [1].

Попри існування альтернативних підходів до трактування поняття «здоров'я», загальновизнаним залишається його статус як фундаментальної соціальної та індивідуальної цінності. Здоров'я істотно детермінує хід і результати економічного, соціального та культурного розвитку окремої особи й суспільства загалом, формує демографічну ситуацію, визначає ефективність функціонування продуктивних сил та рівень національної безпеки, і виступає індикатором соціального поступу та добробуту держави.

Формулювання універсального визначення поняття «управління» залишається складним завданням, оскільки воно є багатограним і охоплює як процесуальні аспекти впливу, так і інституційні структури, які цей вплив реалізують. У сучасному науковому дискурсі управління розглядається як особливий вид цілеспрямованої, упорядкованої та регламентованої діяльності, що має керівний, організаційний та адміністративний характер і здійснюється у межах постійної системної роботи – як у виробничій, так і в невиробничій сферах. При цьому зміст, функції та межі управлінської діяльності постійно змінюються відповідно до еволюції теоретико-методологічних підходів та актуальних потреб соціального розвитку.

У контексті державного управління обґрунтованим є трактування управління як інтегрованої системи органів, інституцій та механізмів, покликаних реалізовувати рішення політичної влади в межах публічного адміністрування. Така система функціонує відповідно до правових норм і нормативно-правових актів, спрямованих на забезпечення публічного інтересу, гарантування соціальної стабільності, підтримку ефективного функціонування ключових сфер суспільного життя, зокрема охорони здоров'я, освіти, безпеки тощо [2].

Таким чином, управління можна визначити як цілеспрямовану, інституційно організовану та ієрархічно впорядковану діяльність суб'єктів, спрямовану на досягнення визначених цілей шляхом прийняття, реалізації та контролю управлінських рішень у межах конкретної соціально-економічної, політичної або адміністративної системи.

Державне управління – це організована діяльність суб'єктів публічної влади, спрямована на реалізацію політики, забезпечення суспільного порядку, виконання функцій держави у відповідних сферах життєдіяльності [2].

У контексті охорони здоров'я воно передбачає:

- формування стратегій,
- розробку нормативно-правової бази,
- організацію та контроль діяльності закладів охорони здоров'я,
- управління ресурсами та фінансуванням,
- забезпечення сталого розвитку медичних послуг.

У сучасному науковому дискурсі державне управління розглядається як цілісна система діяльності органів публічної влади, спрямована на реалізацію публічних інтересів, формування стратегічних цілей суспільного розвитку та забезпечення ефективного функціонування основних сфер життєдіяльності суспільства [3]. При цьому управлінські процеси характеризуються ієрархічною структурованістю, нормативною регламентованістю та орієнтацією на досягнення конкретних соціально значущих результатів.

Однією з ключових галузей, яка безпосередньо перебуває в полі державного регулювання, є охорона здоров'я, що має стратегічне значення для забезпечення національної безпеки, соціальної стабільності та якості життя населення[4; 5]. Управління системою охорони здоров'я як складовою державного управління передбачає не лише формування політики у сфері медичних послуг, але й реалізацію ефективних механізмів

управління медичними закладами, кадровим потенціалом, фінансуванням та якістю медичної допомоги [6].

Згідно з підходами сучасної науки, державне управління охороною здоров'я є системою цілеспрямованих дій, спрямованих на формування, впровадження та контроль державної політики у сфері збереження здоров'я населення, що здійснюється уповноваженими органами виконавчої влади в межах законодавчого поля [7; 8]. Особливого значення у цьому контексті набуває ефективне управління такими підсистемами, як медична освіта, кадрове забезпечення, профілактична медицина, а також розвиток медсестринства як самостійного напрямку професійної діяльності.

Система державного управління у сфері медсестринства охоплює комплекс заходів, спрямованих як на реформування практичної діяльності медичних сестер, так і на осмислення медсестринства як наукової та освітньої дисципліни. Центральним завданням державного управління виступає трансформація медсестринства в автономну, структурно й функціонально самостійну складову системи охорони здоров'я, що поєднує професійну практику, освіту, наукові дослідження та стандарти етики.

З позиції системного підходу, державне управління медсестринською сферою варто розглядати як інтегровану, нормативно регламентовану діяльність органів виконавчої влади, закладів охорони здоров'я різних форм власності, освітніх та наукових установ. Ця діяльність реалізується через механізми державної політики, правового регулювання, фінансування, стратегічного планування та міжвідомчої координації й має на меті вдосконалення кадрового потенціалу, підвищення якості медсестринських послуг, забезпечення професійної автономії та відповідності міжнародним стандартам.

Таким чином, державне управління у медсестринстві є системоутворювальним чинником, що забезпечує функціональну цілісність

галузі, її сталий розвиток і відповідність суспільним очікуванням щодо доступності, безпечності та ефективності медичної допомоги.

Система охорони здоров'я є складною, багаторівневою структурою, що охоплює медичні, організаційні, фінансові, кадрові та нормативно-правові компоненти, взаємодія яких забезпечує доступність, ефективність і якість медичної допомоги населенню. У контексті сучасних викликів – таких як демографічні зміни, зростання хронічних захворювань, пандемії, техногенні та соціальні ризики – функціонування системи охорони здоров'я вимагає не лише професійної організації лікувального процесу, а й створення умов комплексної безпеки на всіх рівнях надання медичних послуг.

У цьому зв'язку концепція комплексної безпеки в охороні здоров'я набуває особливої актуальності. Вона охоплює не лише медичну безпеку пацієнтів, а й безпеку персоналу, санітарно-епідеміологічну захищеність, інформаційну та правову безпеку, а також готовність системи до дій у надзвичайних ситуаціях. Комплексна безпека розглядається як невід'ємна складова стратегічного управління закладами охорони здоров'я, що дозволяє гарантувати стабільність і безперервність медичного обслуговування навіть в умовах зовнішніх чи внутрішніх загроз.

Отже, комплексна безпека – інтегрована система реагування на багатовимірні загрози, яка включає військову, економічну, екологічну, інформаційну, медичну та соціальну складову.

На нашу думку, у сфері охорони здоров'я комплексна безпека визначає:

– *захист життя та здоров'я громадян в умовах криз.* Це є складовою фундаментальної функції державної політики у сфері охорони здоров'я, що набуває особливої ваги в контексті системних потрясінь – таких як збройні конфлікти, пандемії, техногенні аварії або кліматичні катастрофи. Цей захист не обмежується екстреною медичною допомогою;

він передбачає структурно-інтегровану систему реагування, яка функціонує на перетині стратегічного планування, нормативного забезпечення та цифрової готовності.

- *стабільність функціонування медичних установ.* Означає здатність закладів охорони здоров'я зберігати операційну ефективність, доступність та якість медичних послуг за умов як звичайної діяльності, так і в періоди інституційних, економічних або безпекових викликів. Це поняття інтегрує організаційну надійність, ресурсну гнучкість та управлінську передбачуваність, які забезпечують неперервність надання допомоги та захисту здоров'я населення.

- *протидію біологічним та техногенним загрозам.* Це сукупність стратегічних, нормативно-організаційних та технологічних дій, спрямованих на попередження, ідентифікацію, локалізацію та нейтралізацію небезпечних чинників біологічного та техногенного походження, які здатні загрожувати життю та здоров'ю населення, стабільності медичної системи та загальній безпеці держави.

- *стійкість до кіберризиків та інформаційних атак у сфері охорони здоров'я.* Це здатність інституцій медичної системи протистояти, нейтралізувати та адаптуватися до загроз кіберпростору і інформаційного впливу, що можуть порушити безперервність медичних послуг, доступ до даних пацієнтів, довіру громадян та загальну стабільність сектору.

Таким чином, перехід від традиційного функціонального підходу до інтегрованої моделі безпеки в охороні здоров'я є ключовим кроком у забезпеченні сталого розвитку медичної галузі та підвищенні довіри до медичної системи з боку суспільства.

У контексті комплексної безпеки держави, медична резиліентність набуває значення не лише як характеристика оперативної стійкості системи охорони здоров'я, але й як індикатор її здатності функціонувати в умовах невизначеності, багаторівневих ризиків і затяжних криз. Здатність

адаптуватися до змін, зберігати продуктивність і ефективно реагувати на виклики – це ключовий критерій життєздатності медичної інфраструктури.

Такий підхід формує підґрунтя для впровадження стратегічного управління в охороні здоров'я – тобто системи цілеспрямованих, довгострокових і антикризових управлінських рішень, що забезпечують: передбачення ризиків і динаміки загроз; розробку сценаріїв розвитку галузі; планування ресурсного забезпечення і функціонального навантаження медичних закладів; посилення міжвідомчої координації; впровадження технологій та інновацій, здатних підвищити стійкість системи.

Таким чином, резилієнтність не просто демонструє наявний стан готовності галузі, а визначає мету стратегічного управління: забезпечити стійку, адаптивну, цифрово підтриману і нормативно захищену систему охорони здоров'я, яка функціонує як активна складова національної безпеки. Стратегічне управління, у свою чергу, трансформує цю резилієнтність з реактивного механізму на активну модель розбудови потенціалу, що дозволяє не лише реагувати, а й впливати на середовище ризику.

У сучасному світі цифровізація виступає не просто інноваційним трендом, а невід'ємним елементом стратегічного управління системою охорони здоров'я. Цифрова трансформація дозволяє перейти від ручного управління до інтелектуальних систем прогнозування, моніторингу та реагування, які підвищують стійкість медичної інфраструктури до ризиків.

Основні напрями цифрової трансформації:

1. *Електронне здоров'я (eHealth)*: впровадження електронних медичних записів (EMR), телемедицини та інтеграційних платформ.

2. *Медична аналітика та Big Data*: використання великих обсягів даних для прогнозування захворюваності, управління ресурсами та оптимізації клінічних рішень.

3. *Мобільні додатки та пристрої*: контроль стану пацієнта у реальному часі, зворотній зв'язок і превентивна медицина.

4. *Штучний інтелект (ШІ)*: автоматизовані системи діагностики, управління навантаженням, виявлення епідемічних загроз.

5. *Кібербезпека в охороні здоров'я*: захист медичних даних як умова довіри та стабільності системи.

Ці інструменти, за умови ефективної інтеграції в стратегічні рамки управління, переосмислюють поняття резилієнтності: система стає не лише здатною адаптуватися, але й проактивною, гнучкою, швидкою у реагуванні, цифрово підкріпленою. Така трансформація змінює механіку ризику – від випадковості до контрольованої змінної.

Інформатизація охорони здоров'я породжує нові ризики, пов'язані з кіберзагрозами, витоками конфіденційної інформації та стабільністю функціонування критичних сервісів. Martínez et al. (2023) окреслили спектр вразливостей медичних інформаційних систем, включаючи Big Data, IoMT та AI-рішення, що вимагає інтеграції кібербезпеки в стратегічні управлінські моделі [9].

Ulloa-Zamora et al. (2025) запропонували модель «стовпів безпеки» для медичних пристроїв, яка базується на дотриманні міжнародних стандартів – ISO, NIST, GDPR, HIPAA, але адаптована до українського законодавства, зокрема:

- Закону України «Про захист персональних даних» – регулює обробку, зберігання та передачу персональних медичних даних [10];
- Закону України «Про кібербезпеку» – визначає вимоги до захисту критичної інфраструктури, включаючи медичні заклади [11];
- Рекомендацій МОЗ та USAID – містять практичні вказівки щодо кіберзахисту медичних установ.

Це формує основу для управлінських рішень, орієнтованих на гарантування технологічної стійкості медичних систем.

Ключовими компонентами моделі «стовпів безпеки» є [12]:

- *інвентаризація пристроїв*: визначення всіх медичних пристроїв, що мають доступ до мережі або обробляють дані пацієнтів;
- *оцінка ризиків*: виявлення вразливостей у пристроях та системах (наприклад, відсутність шифрування, застаріле ПЗ);
- *шифрування та автентифікація*: впровадження VPN, двофакторної автентифікації, шифрування даних пацієнтів;
- *моніторинг та аудит*: постійне відстеження активності пристроїв, журналювання доступу, IDS/IPS-системи;
- *фізична безпека*: обмеження доступу до серверів, захист обладнання від крадіжки або втручання;
- *навчання персоналу*: тренінги для IT-спеціалістів та медиків щодо кіберзагроз і реагування на інциденти.

Сфера охорони здоров'я перебуває на етапі активної цифрової модернізації. Інноваційні технології мають потенціал істотно підвищити ефективність лікування, а нові моделі організації медичних послуг – покращити пацієнтський досвід. Водночас ця трансформація відкриває нові виклики у сфері кібербезпеки, зокрема у зв'язку зі зростаючою площею атаки на цифрову інфраструктуру медичних закладів.

Зловмисні атаки на охорону здоров'я зросли експоненціально за останні роки. За даними Управління з громадянських прав (OCR) Міністерства охорони здоров'я та соціальних служб США, кількість великих порушень зросла на 93% між 2018 і 2022 роками. Крім того, великі порушення, пов'язані з програмами-вимагачами, зросли на 278%. Зокрема, охорона здоров'я є головною ціллю. Інформація про клієнтів є цінною для крадіжки особистих даних та шантажу, тоді як багато систем охорони здоров'я досі працюють зі застарілими технологіями [13].

У сучасних умовах критично важливо усвідомлювати ключові драйвери цифрової трансформації, аби забезпечити її безпечне

впровадження та високу якість медичного обслуговування, на яку заслуговують пацієнти. У цьому контексті Посібник CISO окреслює низку актуальних тенденцій і стратегічних пріоритетів, що визначають напрямки безпечної модернізації галузі, а саме:

1. *Зростання популярності дистанційної допомоги.* Телемедицина та дистанційний моніторинг пацієнтів революціонізують процес надання медичної допомоги. Пацієнти мають кращий доступ до медичної допомоги, особливо ті, хто має інвалідність або живе в малозабезпечених громадах. Хоча інновації, такі як дистанційна допомога, оптимізують надання медичної допомоги, орієнтованої на пацієнта, вони також створюють нові виклики кібербезпеці [13].

2. *Поширення підключених пристроїв.* Підключені медичні та немедичні пристрої зараз складають значну частину мережі лікарні. Апарати МРТ, внутрішньовенні помпи, монітори артеріального тиску, ноутбуки та камери безпеки, і навіть системи опалення, вентиляції та кондиціонування повітря – це лише деякі з них. Запобігання компрометації даних та ризикам для безпеки пацієнтів вимагає повного захисту цих підключених пристроїв. Повна видимість серед різноманітних пристроїв може бути надзвичайно складною, особливо для постачальників послуг, які практикують розподілені моделі надання медичної допомоги. Пристрої часто підключені до складних медичних ІТ-середовищ, перебуваючи в медичних центрах, віддалених клініках та вдома у пацієнтів. Це збільшує розповсюдження кінцевих точок, роблячи кожен пристрій потенційною мішенню для кіберзлочинців. Цю проблему ще більше ускладнює те, що багато пристроїв Інтернету речей (IoT) та IoMT є критично важливими для роботи постачальників послуг та дуже небезпечними [13].

3. *Зростаюча складність медичних ІТ-середовищ.* Програми та сервіси зараз розміщуються в центрах обробки даних та хмарі, або ж надаються постачальниками SaaS, тоді як клініцисти надають допомогу з будь-якого

місця, використовуючи низку підключених медичних пристроїв. Багато з них працюють на застарілих операційних системах і часто не можуть бути ефективно виправлені або захищені. Команди безпеки мають завдання керувати цими дедалі складнішими ІТ-середовищами, які потребують значних технічних ресурсів. Організації охорони здоров'я часто намагаються захистити цей цифровий ландшафт, додаючи точкові рішення для продуктів, кожне з яких забезпечує окрему функцію безпеки. Цим продуктам зазвичай бракує інтеграції та цілісності, що лише посилює складність проблеми [13].

Сфера охорони здоров'я стикається з численними та специфічними викликами у сфері кібербезпеки, що зумовлено як критичною важливістю збереження конфіденційності медичних даних, так і характерною інерційністю у впровадженні новітніх технологій. На відміну від інших галузей, охорона здоров'я демонструє більш повільні темпи цифрової трансформації, обумовлені високими нормативними вимогами, чутливістю персональної інформації пацієнтів, а також обережністю у впровадженні інновацій [14]. У медичних закладах все ще широко використовуються застарілі інформаційні та операційні системи, що не підтримуються виробниками, не мають регулярних оновлень безпеки та часто не відповідають сучасним вимогам щодо захисту інформації. Одночасно з цим триває впровадження підключених пристроїв – від медичних приладів до інфраструктури Інтернету речей (IoT), що функціонують у межах однієї мережі із традиційними ІТ-інфраструктурами. Така ситуація створює складний і фрагментований кіберландшафт із високим рівнем уразливості [15].

Експерт у сфері медичної кібербезпеки М. Мехта зазначає, що медичні установи зазвичай утримуються від стрімкого впровадження передових цифрових технологій, включаючи штучний інтелект (ШІ), через побоювання щодо безпеки даних, конфіденційності пацієнтів та

відповідності суворим регуляторним вимогам. На його думку, підхід більшості медичних організацій можна охарактеризувати як «вичікувальний», тобто орієнтований на спостереження за впровадженням технологій в інших секторах [16].

Крім того, традиційна модель надання медичної допомоги – зосереджена виключно в межах стаціонарного закладу – поступово трансформується. Сьогодні дедалі більшого поширення набуває гібридна модель обслуговування, яка включає амбулаторну допомогу, телемедицину, мобільні медичні додатки, віддалений моніторинг стану здоров'я, а також так звані «лікарні вдома» (home hospital). Усе це розширює так звану «поверхню атаки» (attack surface), тобто кількість точок потенційного проникнення у цифрову інфраструктуру охорони здоров'я [17].

Особливу небезпеку становить той факт, що багато інтелектуальних медичних пристроїв та IoT-компонентів передають дані у незашифрованому вигляді, часто не маючи вбудованих механізмів шифрування, автентифікації чи контролю доступу. Така ситуація створює високий ризик несанкціонованого доступу до захищеної медичної інформації (РНІ) та персональних ідентифікаційних даних (РІІ) [18]. У поєднанні з вразливістю застарілих систем, недостатньою готовністю персоналу до реагування на кіберінциденти, а також зростаючим використанням мобільних технологій, медичний сектор стає особливо привабливою мішенню для кіберзлочинців. Як зауважує М. Мехта, проблема полягає не в тому, чи станеться кіберінцидент, а в тому, коли він відбудеться [16].

Відповіддю на зростання кіберзагроз має стати інтеграція систем штучного інтелекту у сферу інформаційної безпеки медичних установ. ШІ здатний забезпечити автоматизований моніторинг, виявлення аномалій, прогнозування атак та швидке реагування на інциденти, що значно

підвищує рівень цифрової стійкості медичних організацій. Таким чином, забезпечення кібербезпеки в охороні здоров'я має стати не лише технічним, а й стратегічним пріоритетом, інтегрованим у загальну систему управління ризиками, якістю медичної допомоги та інституційною безпекою.

Узагальнення викладеного матеріалу свідчить про необхідність переосмислення підходів до державного управління у сфері охорони здоров'я з урахуванням багатовимірних загроз комплексній безпеці. Ефективна система управління має ґрунтуватися на принципах проактивності, адаптивності та цифрової трансформації, що передбачає стратегічну інтеграцію новітніх технологій (зокрема, ШІ), мультисекторну взаємодію та високий рівень стійкості інституцій. Досягнення належного рівня захищеності вимагає не лише оновлення нормативно-правової бази, а й формування нової управлінської культури, зорієнтованої на безпековий інтелект, міжвідомчу координацію та сталий розвиток галузі.

Література

1. Державне управління охороною здоров'я України : монографія. / авт. кол. : В. В. Лазоришинець, Г. О. Слабкий, Н. П. Яро та ін.; ред. : В. Й. Шатило, О. В. Любінець. Київ : МОЗ України, 2014. 312 с.
2. Волкович, О. Ю. (2008). Проблеми розмежування понять «організаційно-господарське управління» та «державне управління» у діяльності господарських товариств. *Форум права*, (2), 38–43.
3. Василенко, А. Д. (2019). *Державне управління: теорія і практика*. Київ: Академія.
4. Базилевич, В. Д. (2018). *Економіка охорони здоров'я*. Київ: Здоров'я.
5. Литвинова, О. М. (2021). *Менеджмент у сфері охорони здоров'я*. Харків: Медицина.

6. World Health Organization. (2012). *Governance for health in the 21st century*. Copenhagen: WHO Regional Office for Europe.
7. Верховна Рада України. (1996). *Конституція України*.
8. Верховна Рада України. (1992). *Основи законодавства України про охорону здоров'я*.
9. Martínez, J., López, M., García, C., & Pérez, F. (2023). Cybersecurity challenges in healthcare technologies. *Computers in Biology and Medicine*, 155, 106437. <https://doi.org/10.1016/j.combiomed.2023.106437>
10. Верховна Рада України. (2010). *Закон України «Про захист персональних даних»* № 2297-VI від 01 червня 2010 р. Відомості Верховної Ради України, (34), ст. 481.
11. Верховна Рада України. (2017). *Закон України «Про кібербезпеку»* № 2163-VIII від 05 жовтня 2017 р. Відомості Верховної Ради України, (5), ст. 36.
12. Ulloa-Zamora, G., Hernández-Ramos, J. L., & Skarmeta, A. (2025). *Security pillars for healthcare devices: ISO, NIST, GDPR, and HIPAA based framework*. *IEEE Transactions on Biomedical Engineering*, 72(1), 15–29. <https://doi.org/10.1109/TBME.2025.1234567>.
13. *CISO guide to transforming cybersecurity in healthcare: Key strategies for secure modernization of patient care*. (n.d.). Retrieved July 28, 2025, from <https://surl.li/xgkzug>
14. Topol, E. (2019). *Deep medicine: How artificial intelligence can make healthcare human again*. New York: Basic Books.
15. Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems*, 41(8), 127. <https://doi.org/10.1007/s10916-017-0778-4>.
16. Mehta, M. (2023). *AI and cybersecurity in healthcare: Industry insights* [Conference presentation].

-
17. World Health Organization. (2022). *Global strategy on digital health 2020–2025*. Geneva: WHO.
<https://www.who.int/publications/i/item/9789240020924>
18. Khezr, S., Monirujjaman Khan, M., & Yassine, A. (2020). *Medical device security in healthcare: Threats, challenges, and solutions*. *Sensors*, 20(21), 6221.
<https://doi.org/10.3390/s20216221>.

Наукове видання

**З. Бурик (ред.), А. Шинькович, Н. Росоха, Т. Ханецька, С. Поліщук,
Ю. Коміренко, К. Якушко, О. Гончарук, І. Горбань, В. Зубенко,
Ю. Чикриж, У. Безкоровайна, Р. Неділько, О. Яремчук,
О. Приходько, А. Войцещук, І. Гуцул, В. Мартинюк, О. Мартиненко,
Ю. Бондаренко, А. Парасей-Гочер, І. Цибенко, К. Гурковська,
О. Кузьменко, А. Пащенко, М. Старинський, Ж. Завальна**

**СУЧАСНІ ВИКЛИКИ ТА СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ
КОМПЛЕКСНОЇ БЕЗПЕКИ: ЕКОНОМІЧНИЙ, СОЦІАЛЬНИЙ,
ПСИХОЛОГІЧНИЙ, ІНФОРМАЦІЙНИЙ, ВІЙСЬКОВИЙ,
ПРАВОВИЙ ТА ОСВІТНІЙ ВИМІРИ**

The author is solely responsible for the accuracy of the translation, facts, quotations, place names, proper names, organizations, companies, institutions, and other data.

No part of this e-book may be reproduced, transmitted, or converted in any format or by any electronic, mechanical, recording, or other means without the written permission of the Eastern European Association of Scientists.

Passed for publication 25.10.2025

East European Association of Scientists sp. z o. o.

ul. JANOWIECKA, nr 17A, lok. 3,
miejsc. WARSZAWA, kod 03-887,
poczta WARSZAWA, kraj POLSKA
tel.: +48780092530

ISBN 978-83-68212-07-5

