МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«Харківський авіаційний інститут»

**ЛАСУКОВ Олександр Євгенійович**

УДК 351.86:004.056(477)

# МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

25.00.02 – механізми державного управління

**АВТОРЕФЕРАТ**
дисертації на здобуття наукового ступеня
кандидата наук з державного управління

Харків – 2026

Дисертацією є рукопис.
Робота виконана в Національному університеті цивільного захисту України.

Науковий керівник – доктор наук з державного управління, професор
**КРЮКОВ Олексій Ігорович**
Національний аерокосмічний університет «Харківський авіаційний інститут»,
науковий співробітник відділу забезпечення наукової діяльності.

Офіційні опоненти: доктор наук з державного управління, доцент
**СПОРИШЕВ Костянтин Олександрович**
Національна академія Національної гвардії України,
заступник начальника навчально-наукового інституту підготовки керівних кадрів з наукової роботи – начальник науково-дослідної лабораторії будівництва та оперативного застосування;

кандидат наук державного управління
**ВЕРБОВЕНКО Олександр Павлович**
Центральне управління цивільно-військового співробітництва Генерального штабу Збройних Сил України, заступник начальника.

Захист відбудеться «18» грудня 2026 року о 14 годині на засіданні спеціалізованої вченої ради Д 64.062.09 Національного аерокосмічного університету «Харківській авіаційний інститут» за адресою: 61070, м. Харків, вул. Вадима Манька, 17.

З дисертацією можна ознайомитись в науково-технічній бібліотеці Національного аерокосмічного університету «Харківський авіаційний інститут» за адресою: 61070, м. Харків, вул. Вадима Манька, 17.

Автореферат розісланий «18» листопада 2026 р.

Вчений секретар
спеціалізованої вченої ради Надія КАРПЕКО

## ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність теми дослідження.** Розвиток інформаційного суспільства та стрімка цифровізація державного управління зумовили якісні зміни у характері загроз національній безпеці сучасних держав. Кіберпростір перетворився на повноцінний театр воєнних дій, у якому поряд із традиційними збройними протистояннями розгортаються масштабні операції, спрямовані на ураження критичної інфраструктури, дезорганізацію систем державного управління та підрив обороноздатності країни. Для України ця проблематика набула особливої гостроти в умовах повномасштабної збройної агресії російської федерації, яка супроводжується безпрецедентним за інтенсивністю кібернаступом на інформаційні системи органів сектору безпеки і оборони.

Актуальність теми обумовлена низкою взаємопов'язаних чинників. По-перше, інформаційні системи органів сектору безпеки і оборони України функціонують в умовах постійного кібернетичного тиску з боку противника, що висуває принципово нові вимоги до механізмів їх захисту на рівні державного управління. По-друге, наявна інституційна архітектура управління кібербезпекою характеризується розмитістю відповідальності між ключовими суб'єктами – Державною службою спеціального зв'язку та захисту інформації України, Службою безпеки України, Національним координаційним центром кібербезпеки при РНБО – що знижує ефективність координації та оперативність реагування на кіберінциденти. По-третє, чинна нормативно-правова база у сфері кібербезпеки, сформована переважно до початку повномасштабного вторгнення, потребує суттєвого вдосконалення з урахуванням реалій воєнного часу та вимог євроатлантичної інтеграції. По-четверте, відсутній дієвий механізм оцінки ефективності кіберзахисту інформаційних систем органів сектору безпеки і оборони на управлінському рівні, що унеможливлює прийняття обґрунтованих управлінських рішень щодо розподілу ресурсів та визначення пріоритетів.

Незважаючи на значний обсяг наукових праць з проблематики державного управління у сфері кібербезпеки, механізми державного управління кібербезпекою саме інформаційних систем органів сектору безпеки і оборони в умовах воєнного стану залишаються недостатньо дослідженими. Відсутня цілісна концептуальна модель такого управління, не сформована система вимірюваних індикаторів оцінки його ефективності, потребує наукового обґрунтування механізм адаптації стандартів НАТО до українських реалій. Це й зумовило вибір теми дисертаційної роботи, її мету і завдання.

Актуальність теми посилюється й євроатлантичним вектором розвитку України: імплементація стандартів НАТО у сфері кібербезпеки з обов'язкового орієнтира перетворилася на практичну умову поглиблення оборонної інтеграції, що потребує не просто декларативного визнання відповідних стандартів, а розробки дієвого управлінського механізму їх поетапного впровадження в умовах обмежених ресурсів воєнного часу. Водночас накопичений з початку повномасштабного вторгнення унікальний досвід кібероборони України – зокрема у протидії атакам на об'єкти критичної інфраструктури та інформаційні

системи органів сектору безпеки і оборони – потребує наукового осмислення та систематизації для того, щоб не залишитися лише сукупністю розрізнених оперативних практик, а стати основою сталої інституційної спроможності держави.

Теоретичне підґрунтя дослідження склали праці вітчизняних учених з проблематики державного управління у сфері кібербезпеки, інформаційної та національної безпеки В. Антонюк, В. Баштанник, С. Бєлай, О. Бондаренко, Д. Вєдєнєєв, О. Вербовенко, Т. Воропаєва, В. Горбулін, О. Довгань, С. Домбровська, Ю. Древаль, О. Копанчук, О. Кравчук, С. Крук, О. Крюков, О. Курбан, Є. Магда, О. Машков, О. Мережко, Н. Нижник, О. Пархоменко-Куцевіл, А. Помаза-Пономаренко, С. Порока, Г. Почепцов, В. Палюх, Р. Прав, Р. Примуш, О. Радченко, А. Рубан, І. Рущенко, Г. Ситник, В. Скуратівський, В. Степанов, В. Торічний, Е. Щепанський, Т. Яровий та ін

Сутність, структура та інші аспекти державного управління у сфері розвитку цифрових технологій неодноразово досліджувались у працях зарубіжних науковців Л. Антопулос, С. Арадау, Е. Аркін, У. Бека, З. Бжезінського, С. Бергера, С. Брозе, Д. Бетца, А. Волферса, М. Веле, М. Гарсії-Алонсо, С. Гібба, А. Гідденса, Р. Гранта, М. Девідсона, Д. Деннінга, П. Едвардса, А. Едельштайн, І. Кекіш, Т. Келлі, М. Клавер, А. Кларка, К. Крісті, Б. Маби, Ф. Майлза, В. Мустаки, Н. Наєма, Дж. Найа, Т. Накаї, П. Норвіга, М. О'Коннелла, Дж. Паджетт, Дж. Паркера, І. Пула, С. Рассела, С. Рінальді, Дж. Розе, С. Родан, М. Ронки, С. Сассен, Т. Стівенса, Е. Тоффлера, М. Хоровітц, Ф. Хоффмана, П. Шарре, Дж. Шуха, Т. Яновскі та ін.

Водночас питання цілісного, інтегрованого механізму державного управління кібербезпекою саме інформаційних систем органів сектору безпеки і оборони України в умовах збройної агресії, що поєднував би інституційний, індикативний та євроатлантичний виміри, дотепер не було предметом самостійного наукового дослідження.

**Зв'язок роботи з науковими програмами, планами, темами**. Дисертаційне дослідження проведено в межах науково-дослідних робіт, які виконувались Національним університетом цивільного захисту України, а саме: за темою «Розробка наукових основ державного управління у сфері безпеки ринку соціально-економічних послуг України з точки зору цивільного захисту» (ДР № 0115U002035), у межах якої здобувачем визначено засади формування кібербезпеки інформаційних систем органів сектору безпеки і оборони України.

**Мета та завдання дослідження**. Метою дослідження є визначення науково-теоретичних засад та розробка практичних рекомендацій з удосконалення механізмів державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України в умовах сучасних безпекових викликів. Відповідно до сформульованої мети необхідно вирішити такі завдання дослідження:

– дослідити теоретичні засади державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони та уточнити понятійно-категоріальний апарат у відповідній сфері;

– класифікувати механізми державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони та проаналізувати стан їх нормативно-правового забезпечення, визначивши напрями його вдосконалення в умовах воєнного стану та євроатлантичної інтеграції;

– проаналізувати інституційну систему суб'єктів державного управління кібербезпекою сектору безпеки і оборони, виявити проблеми їх координації та здійснити оцінку ефективності існуючих механізмів кіберзахисту інформаційних систем;

– узагальнити зарубіжний досвід державного управління кібербезпекою у секторі безпеки і оборони та обґрунтувати можливості і межі його адаптації до українських реалій;

– розробити концептуальну модель механізму державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України та сформувати систему індикаторів оцінки її ефективності;

– обґрунтувати механізм імплементації стандартів НАТО у сфері кібербезпеки до умов українського сектору безпеки і оборони з урахуванням досвіду, набутого в умовах повномасштабного збройного конфлікту.

**Об'єктом дослідження** є система державного управління кібербезпекою в Україні.

**Предметом дослідження** є механізми державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України.

**Методи дослідження**. Методологічну основу дисертації становить сукупність загальнонаукових та спеціальних методів наукового пізнання. Системний метод застосовано для дослідження механізмів державного управління кібербезпекою як цілісної системи взаємопов'язаних елементів. Структурно-функціональний аналіз використано при дослідженні інституційної архітектури управління кібербезпекою сектору безпеки і оборони. Порівняльно-правовий метод застосовано при аналізі зарубіжного досвіду та міжнародних стандартів у відповідній сфері. Метод моделювання використано при розробці концептуальної моделі механізму державного управління кібербезпекою. Метод кейс-аналізу застосовано для поглибленого дослідження знакових кіберінцидентів 2022–2025 років, контент-аналіз – при опрацюванні стратегічних і нормативно-правових документів та звітів CERT-UA, статистичний метод – для аналізу динаміки кіберінцидентів.

Застосування SWOT-аналізу дало змогу структуровано зіставити сильні й слабкі сторони чинної системи державного управління кібербезпекою з можливостями та загрозами, зумовленими зовнішнім безпековим середовищем, і на цій основі обґрунтувати пріоритетність запропонованих напрямів удосконалення. Метод експертних оцінок у поєднанні з методом аналізу ієрархій покладено в основу методики визначення вагових коефіцієнтів індикаторів та їх агрегування в інтегральний індекс, що дає змогу забезпечити об'єктивність та легітимність результувальної оцінки за відсутності достатнього обсягу історичних даних, характерних для відносно нової предметної області.

Інформаційно-фактологічною базою дослідження є: закони України, укази Президента України, нормативні акти Кабінету Міністрів України, стратегічні документи та звіти органів сектору безпеки і оборони, щорічні звіти ДССЗЗІ та CERT-UA про кіберінциденти за 2022–2025 роки, аналітичні матеріали НАТО, ЄС і ENISA, звіти міжнародних дослідницьких груп щодо кібероперацій проти України, а також матеріали стратегічних дискусій НКЦК щодо нової Стратегії кібербезпеки України.

**Наукова новизна одержаних результатів** полягає у вирішенні наукового завдання щодо розвитку теоретичних засад та обґрунтування науково-прикладних рекомендацій з удосконалення механізмів державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України. Найсуттєвіші результати дисертаційного дослідження, які містять наукову новизну, полягають у тому, що:

*вперше:*

- розроблено концептуальну модель механізму державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України, яка, на відміну від поширених у науці державного управління блокових моделей описового характеру, має три принципові відмінності: по-перше, визначає кіберстійкість, а не абсолютну захищеність, цільовою категорією управління; по-друге, добудовує контур державного управління до замкненого – інтегрує цільовий, суб'єктний, функціональний, забезпечувальний та результуючий блоки за кібернетичною логікою вимірювання стану об'єкта та коригувального впливу, для чого в межах моделі сформовано систему з двадцяти базових індикаторів оцінки ефективності кіберзахисту на управлінському рівні у п'яти групах, агрегованих у зважений інтегральний індекс кіберзахищеності сектору безпеки і оборони, з режимами оцінювання мирного часу, воєнного стану та відновлення і чотирма пороговими рівнями, прив'язаними до типових управлінських рішень; по-третє, передбачає інституційні новації у вигляді єдиного національного центру кіберстійкості з операційними повноваженнями, унормованих Кіберсил Збройних Сил України та міжвідомчого національного кіберрезерву;

*удосконалено:*

- теоретичні засади державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони: поглиблено наукове обґрунтування співвідношення понять «інформаційна безпека», «кібербезпека», «кіберзахист» і «захист інформації» та доведено, що кібербезпека зазначених систем має розглядатися у державно-управлінському, а не суто технічному вимірі – як стан їх захищеності, що досягається цілеспрямованим управлінським впливом уповноважених суб'єктів держави;
- класифікацію механізмів державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони – за природою управлінського впливу, рівнем управління та функціональним призначенням, а також систематизовано стан їх нормативно-правового забезпечення з виокремленням п'яти історичних етапів його становлення та шести рівнів

правового регулювання, що уможливило обґрунтування пріоритетних напрямів удосконалення нормативно-правової бази;

*набули подальшого розвитку:*

- наукові положення щодо інституційної системи суб'єктів державного управління кібербезпекою сектору безпеки і оборони України та механізмів координації між ними: встановлено її чотирирівневу архітектуру (стратегічний, координаційний, операційний, об'єктовий рівні) і виявлено системні проблеми розмежування повноважень, фрагментації центрів оперативного реагування та інституційної слабкості координаційного органу, які знижують дієвість наявних механізмів кіберзахисту;
- методологічні підходи до адаптації зарубіжного досвіду державного управління кібербезпекою у секторі безпеки і оборони до українських реалій: на основі узагальнення практики Сполучених Штатів Америки, Великої Британії, Німеччини, Франції, Польщі, Естонії, Ізраїлю та Нідерландів обґрунтовано модель вибіркової адаптації інституційних принципів із одночасним збереженням та інституціоналізацією унікальних напрацювань воєнного часу;
- механізм імплементації стандартів НАТО у сфері кібербезпеки до умов українського сектору безпеки і оборони, якому надано вигляду повторюваного п'ятиетапного циклу (інвентаризація і моніторинг – пріоритезація – транспозиція – впровадження – оцінювання сумісності) з двостороннім контуром обміну набутим в умовах повномасштабної війни досвідом кібероборони з партнерами.

**Практичне значення одержаних результатів**. Результати дослідження можуть бути безпосередньо використані: органами державної влади – при вдосконаленні нормативно-правової бази у сфері кібербезпеки; Національним координаційним центром кібербезпеки при РНБО – при вдосконаленні координаційних механізмів між суб'єктами забезпечення кібербезпеки сектору безпеки і оборони; органами сектору безпеки і оборони – при організації системи кіберзахисту інформаційних систем; закладами вищої освіти – у навчальному процесі з підготовки фахівців у сфері державного управління та кібербезпеки.

Результати дослідження впроваджено у діяльність: Департаменту захисту критичної інфраструктури ДКІ Адміністрації Держспецзв’язку (довідка № 07/03-10919/2026 від 21.09.2026); Головного центру підготовки Державної прикордонної служби України (довідка від 21.05.2026); та в освітній процес Національної академії національної гвардії України (акт про впровадження від 12.06.2026). Матеріали дисертації також використовуються в освітньому процесі при підготовці магістрів публічного управління та адміністрування в Національного університеті цивільного захисту України.

**Особистий внесок здобувача.** Дисертаційне дослідження виконано здобувачем самостійно. Теоретичні положення, практичні рекомендації, висновки та пропозиції, у тому числі й ті, що характеризують наукову новизну, отримані здобувачем особисто в ході дослідження.

**Апробація результатів дисертації**. Основні положення й результати

дисертації доповідались і обговорювались на конференціях і семінарах, зокрема: на науково-практичній конференції «Стратегічний розвиток держави, науки та освіти в умовах сучасних викликів» (м. Львів, 2026); Міжнародній науково-практичній інтернет-конференції «Публічне управління у сфері цивільного захисту: освіта, наука, практика» (м. Харків, 2023); Міжнародній науково-практичній інтернет-конференції «Публічне управління у сфері цивільного захисту: освіта, наука, практика» (м. Харків, 2024).

**Публікації.** Основні положення дисертаційної роботи опубліковано в 9 наукових працях: 5 статтях у наукових фахових виданнях України, 4 тезах матеріалах наукової конференції. Загальний обсяг публікацій – 2,3 авт. арк.

**Структура та обсяг дисертації.** Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, додатків. Дисертація містить 7 таблиць та 4 рисунки. Загальний обсяг дисертації становить 211 сторінок, з яких 174 сторінки – основний текст. Список використаних джерел включає 233 найменування.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дослідження, зумовлену безпрецедентним за інтенсивністю кібернетичним тиском на інформаційні системи органів сектору безпеки і оборони України в умовах повномасштабної збройної агресії; з'ясовано зв'язок роботи із Стратегією кібербезпеки України та Законом України «Про основні засади забезпечення кібербезпеки України»; визначено мету, шість завдань, об'єкт і предмет дослідження; охарактеризовано методи дослідження; розкрито наукову новизну і практичне значення одержаних результатів; наведено відомості про їх апробацію та оприлюднення.

**У першому розділі** – «*Теоретичні засади державного управління кібербезпекою інформаційних систем сектору безпеки і оборони*» – простежено ґенезу поняття кібербезпеки від суто технічної категорії захисту комп'ютерних систем до комплексної категорії державного управління та національної безпеки, що пройшла етапи становлення, формування, інституціоналізації та стратегічної зрілості. Уточнено співвідношення понять «інформаційна безпека», «кібербезпека», «кіберзахист» та «захист інформації»; обґрунтовано, що стосовно інформаційних систем органів сектору безпеки і оборони кібербезпека має розглядатися у державно-управлінському вимірі – як стан захищеності, що досягається цілеспрямованим управлінським впливом уповноважених суб'єктів держави. Обґрунтовано розширення класичної тріади «конфіденційність – цілісність – доступність» для сектору безпеки і оборони двома компонентами – стійкістю (здатність до деградованого функціонування та швидкого відновлення) та інтероперабельністю (сумісність із системами партнерів по НАТО) – і на цій основі сформульовано авторське визначення кібербезпеки інформаційних систем органів сектору безпеки і оборони як системи управлінських відносин. Доведено, що специфіка таких інформаційних систем (критичність для обороноздатності, обробка інформації з обмеженим

доступом, функціонування в умовах цілеспрямованого впливу противника) зумовлює підвищені вимоги до механізмів державного управління їх кібербезпекою порівняно із цивільними системами.

Проведено періодизацію розвитку кібербезпеки як категорії державного управління, у межах якої виокремлено етап становлення (переважно технічне трактування захисту автоматизованих систем), етап формування (перші спроби нормативного визначення кібербезпеки як самостійного об'єкта державної політики), етап інституціоналізації (створення спеціалізованих органів та прийняття базового законодавства) та етап стратегічної зрілості, який розпочався з посиленням гібридних загроз після 2014 року і набув особливої динаміки в умовах повномасштабної збройної агресії. Обґрунтовано, що саме на етапі стратегічної зрілості відбувається остаточне закріплення кібербезпеки інформаційних систем сектору безпеки і оборони як окремого об'єкта державного управління зі специфічним суб'єктним складом, інструментарієм і критеріями результативності.

Здійснено класифікацію механізмів державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони за природою управлінського впливу – шість типів замість традиційних чотирьох (правові, організаційні, економічні, технічні, кадрові, інформаційно-комунікативні), з обґрунтуванням виокремлення технічних, кадрових та інформаційно-комунікативних механізмів як самостійних для досліджуваної сфери, за рівнем управління (загальнодержавний, секторальний, відомчий, об'єктовий) та за функціональним призначенням (механізми запобігання, виявлення, реагування, відновлення, стримування). На цій основі систематизовано стан нормативно-правового забезпечення кібербезпеки органів сектору безпеки і оборони України: виокремлено п'ять етапів його становлення та шість рівнів регулювання – конституційний, законодавчий, стратегічний, підзаконний, відомчий і міжнародно-правовий.

Порівняльний аналіз законодавства України з підходами ЄС засвідчив, що вітчизняна нормативно-правова база у сфері кібербезпеки в цілому відповідає загальній логіці Директиви NIS2 щодо визначення кола суб'єктів критичної інфраструктури та вимог до управління ризиками, проте істотно відстає в частині деталізації обов'язкових технічних і організаційних заходів безпеки, строків повідомлення про інциденти та механізмів незалежного нагляду за дотриманням вимог. Встановлено, що для інформаційних систем органів сектору безпеки і оборони додатковим ускладнювальним фактором є накладення режиму державної таємниці на значну частину відповідної інформації, що вимагає розроблення спеціальних, відмінних від цивільного сектору процедур звітності про кіберінциденти, які одночасно забезпечували б оперативність державного реагування і збереження таємності чутливих відомостей.

Виявлено системні проблеми нормативно-правового поля: рамковість базового закону, термінологічну неузгодженість, дублювання повноважень між суб'єктами забезпечення кібербезпеки, невідповідність успадкованої моделі захисту інформації сучасним технологічним реаліям, недостатню адаптованість

законодавства до умов воєнного стану та незавершеність гармонізації з правом ЄС і стандартами НАТО. Показано, що Закон України від 27 березня 2025 року № 4336-IX, який запровадив національну систему реагування на кіберінциденти, обов'язкові підрозділи кіберзахисту та керівників з питань кібербезпеки і започаткував відхід від моделі комплексних систем захисту інформації, лише частково пом'якшив ці проблеми для цивільного сегмента, не створивши спеціального режиму для сектору безпеки і оборони; законопроєкт «Про Кіберсили Збройних Сил України» (№ 12349) прийнято за основу у жовтні 2025 року, а проєкт нової Стратегії кібербезпеки України представлено НКЦК у червні 2026 року. Обґрунтовано пріоритетні напрями вдосконалення нормативно-правової бази, зокрема системне оновлення базового законодавства із закріпленням ризик-орієнтованого підходу, законодавче унормування кібероборони та статусу кіберсил, імплементацію Директиви NIS2 та створення спеціального правового режиму функціонування національної системи кібербезпеки в умовах воєнного стану.

Здійснено структурно-функціональний аналіз взаємозв'язку кібербезпеки з іншими видами безпеки, що входять до складу національної безпеки держави, зокрема з інформаційною, воєнною та економічною безпекою. Обґрунтовано, що кібербезпека інформаційних систем органів сектору безпеки і оборони одночасно є самостійним об'єктом державного управління та наскрізною умовою ефективного функціонування решти складових нацбезпеки, адже порушення кіберзахищеності систем управління військами, розвідки чи прикордонного контролю здатне паралізувати виконання завдань відповідних органів навіть за відсутності прямого фізичного впливу на особовий склад чи техніку.

Досліджено еволюцію доктринальних підходів до розуміння кібербезпеки як об'єкта державного управління – від вузькотехнічного трактування через призму захисту окремих інформаційних систем до комплексного розуміння кіберстійкості як властивості всієї соціотехнічної системи сектору безпеки і оборони. Обґрунтовано, що для інформаційних систем органів сектору безпеки і оборони визначальною є здатність системи зберігати функціональність та швидко відновлюватися після кібератаки в умовах безперервного впливу супротивника, що потребує зміщення акценту державно-управлінського впливу на комплексне управління кіберстійкістю у динаміці.

Охарактеризовано штучний інтелект як наскрізний фактор трансформації державного управління кібербезпекою. Обґрунтовано подвійну природу цього фактора: з одного боку, зловмисники дедалі активніше використовують генеративні моделі для автоматизації розвідки та створення шкідливого коду, з іншого – алгоритми машинного навчання відкривають нові можливості виявлення аномалій та автоматизованого реагування на кіберінциденти. Доведено управлінський, а не суто технологічний вимір цієї проблематики – з урахуванням підходів Національної комісії з питань штучного інтелекту у сфері безпеки США та Регламенту ЄС про штучний інтелект – і обґрунтовано необхідність окремого кадрового переоснащення органів сектору безпеки і оборони для розбудови компетентностей з управління алгоритмічними ризиками.

**У другому розділі** – «*Аналіз стану державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони*» – досліджено інституційну систему суб'єктів управління кібербезпекою зазначеного сектору. Показано, що чотирирівнева інституційна система (стратегічний, координаційний, операційний та об'єктовий рівні) є функціонально повною (рис. 1), однак її ефективність знижується через розмитість розмежування повноважень, множинність центрів оперативного реагування за відсутності єдиного центру управління, відомчу закритість, інституційну слабкість координаційного механізму, кадровий дефіцит та недостатню цивільно-військову інтеграцію.

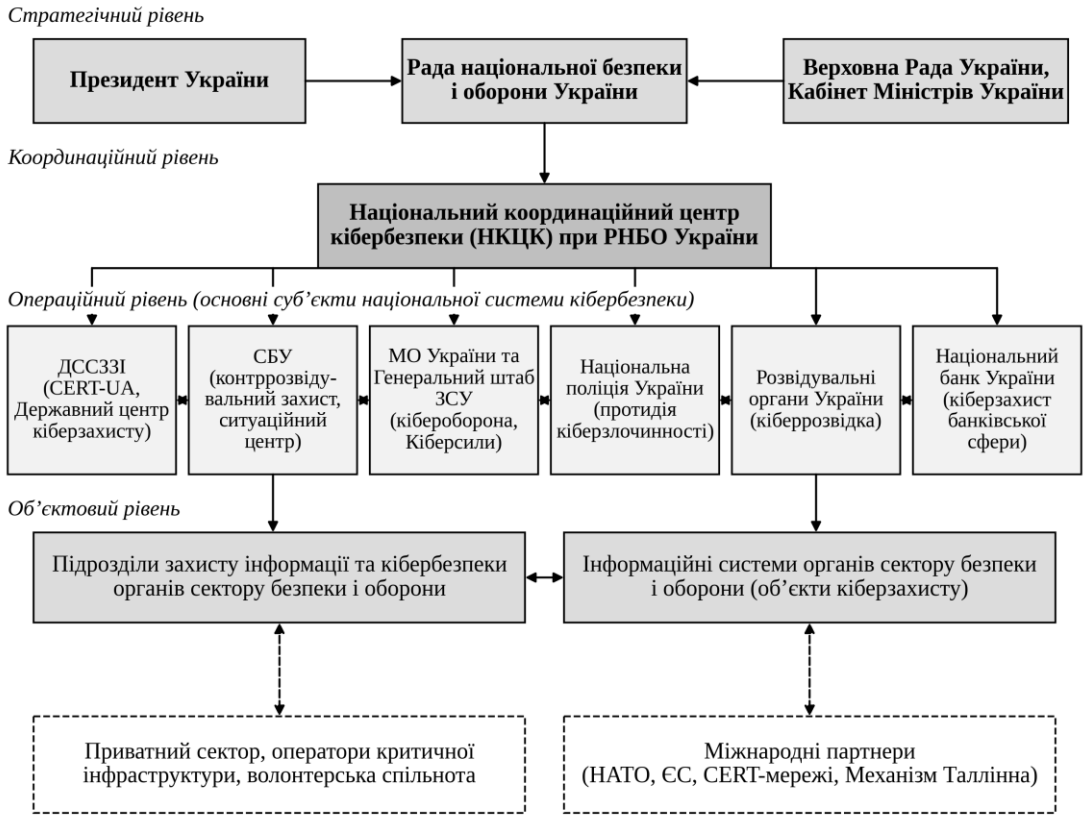



Рис. 1. Інституційна система суб'єктів державного управління кібербезпекою сектору безпеки і оборони України

Здійснено оцінку ефективності існуючих механізмів кіберзахисту інформаційних систем сектору безпеки і оборони в умовах повномасштабної збройної агресії. Встановлено, що продемонстрована в умовах безпрецедентної кібернетичної агресії стратегічна стійкість національної системи кібербезпеки значною мірою ґрунтується на надзвичайних заходах, зовнішній підтримці та неформальній взаємодії, а не на усталеній інституційній спроможності; найслабшими ланками визначено кадрове забезпечення, неповноту моніторингу, фрагментацію координації реагування та відсутність системи вимірювання ефективності кіберзахисту на управлінському рівні.

Здійснено аналіз кадрового забезпечення органів, що виконують функції кіберзахисту в секторі безпеки і оборони. З'ясовано, що дефіцит кваліфікованих

фахівців з кібербезпеки, потреба в яких оцінюється у тисячі осіб, посилюється конкуренцією з боку приватного сектору та союзницьких структур, а грошове забезпечення на державній та військовій службі у кілька разів поступається ринковим ставкам, що зумовлює «інверсію досвіду» – відтік найдосвідченіших фахівців саме в момент піку їх кваліфікації. Обґрунтовано, що без цільових кадрових програм – національної рамки кваліфікацій кібербезпеки, диференційованого грошового забезпечення дефіцитних спеціальностей, партнерства із закладами вищої освіти та використання служби у кіберпідрозділах як освітньої траєкторії – інституційні та нормативно-правові вдосконалення не даватимуть повного ефекту через відсутність кадрової спроможності для їх практичної реалізації.

Проаналізовано динаміку кіберінцидентів, опрацьованих CERT-UA у 2022–2025 роках: їх кількість зросла з близько 2,1 тис. у 2022 році до 2 543 у 2023, 4 315 у 2024 та 5 927 у 2025 році (приріст 37,4 відсотка за рік), причому на сектор безпеки і оборони у 2025 році припало 1 039 інцидентів (17,5 відсотка), а кількість фішингових кампаній подвоїлася (з 843 до 1 727). Встановлено структурний зсув у бік фішингу та компрометації облікових записів, що свідчить: основним вектором проникнення в інформаційні системи сектору стає не периметр мережі, а кінцевий користувач, – спостереження, яке має принципове значення для визначення пріоритетів кадрових та інформаційно-комунікативних механізмів і перегляду розподілу ресурсів кіберзахисту в бік безперервного моніторингу поведінкових аномалій.

Методом кейс-аналізу поглиблено досліджено три резонансні кіберінциденти, що виконали функцію стрес-тесту національної системи кібербезпеки: атаку на супутникову мережу KA-SAT (24 лютого 2022 року, шкідливе програмне забезпечення AcidRain, з наслідками для близько 5,8 тис. вітрогенераторів у Німеччині); атаку на оператора «Київстар» (грудень 2023 року, угруповання Sandworm, порушення зв'язку близько 24 млн абонентів); та атаку на державні реєстри Міністерства юстиції України (грудень 2024 року, компрометація близько 60 реєстрів), – а також четвертий, безпосередньо пов'язаний з предметом дослідження, масив інцидентів: цільові кампанії 2022–2025 років проти користувачів бойових інформаційних систем та захищених месенджерів Сил оборони (кампанія проти користувачів системи DELTA, SickSync угруповання UAC-0020, операції проти користувачів Signal із приманкою під застосунок «Кропива», кампанія UAC-0200). Встановлено, що для бойових інформаційних систем периметр захисту фактично збігається з особистим пристроєм і обліковим записом окремого військовослужбовця, а отже технічні механізми не дають ефекту без кадрових та інформаційно-комунікативних. На основі цих кейсів та SWOT-аналізу стану наявних механізмів верифіковано практичну застосовність запропонованих у третьому розділі концептуальної моделі та системи індикаторів оцінки ефективності кіберзахисту.

Узагальнено досвід державного управління кібербезпекою у секторі безпеки і оборони восьми держав – США, Великої Британії, Німеччини, Франції, Польщі, Естонії, Ізраїлю та Нідерландів – а також інституційних

платформ НАТО і ЄС. Виявлено стійкі закономірності ефективних національних моделей: наявність єдиного національного органу кібербезпеки; інституціоналізацію військових кіберспроможностей у формі окремих командувань або видів збройних сил; систематичне державно-приватне партнерство; ризик-орієнтоване управління на основі вимірюваних індикаторів; волонтерські кіберрезерви та глибоку міжнародну інтеграцію. Обґрунтовано модель вибіркової адаптації, яка передбачає запозичення інституційних принципів із одночасним збереженням та інституціоналізацією унікальних українських напрацювань воєнного часу.

Здійснено порівняльний аналіз інституційних моделей координації кібербезпеки за критеріями централізації повноважень, обсягу залучення приватного сектору, наявності окремих військових кіберкомандувань та рівня використання волонтерських кіберрезервів. Встановлено, що держави з високим рівнем зовнішньої безпекової загрози (Естонія, Ізраїль, Польща) послідовно обирають модель високої централізації прийняття рішень при одночасній децентралізації операційного виконання через галузеві команди реагування, тоді як держави без гострих зовнішніх загроз (окремі країни Західної Європи) можуть дозволити собі більш розподілену, консенсусну модель координації без істотних втрат в ефективності реагування.

Особливу увагу приділено досвіду Естонії як держави, що зазнала масштабної кібератаки 2007 року і на цій основі побудувала одну з найбільш інституційно зрілих систем кібербезпеки в Європі, а також досвіду Ізраїлю, чия модель поєднання централізованого державного управління з високим рівнем залучення приватного сектору й академічної спільноти демонструє високу адаптивність в умовах перманентних безпекових викликів. Порівняльний аналіз засвідчив, що пряме копіювання жодної із зазначених моделей є недоцільним для України через специфіку її безпекового середовища, водночас окремі інституційні рішення – зокрема принцип єдиного центру прийняття рішень та практика регулярного незалежного аудиту кіберзахищеності критичної інфраструктури – є придатними до адаптації без істотних додаткових ресурсних витрат.

Узагальнено також досвід Нідерландів, де розвинена громадянсько орієнтована модель кібербезпеки. Охарактеризовано функції Національного центру кібербезпеки (NCSC-NL) у структурі Національного координаційного центру з протидії тероризму та безпеки, чотири стратегічні напрями Стратегії кібербезпеки Нідерландів на 2022–2028 роки, практику відповідального розкриття вразливостей та діяльність незалежної консультативної Ради з кібербезпеки. Обґрунтовано придатність окремих елементів нідерландської моделі – інституціоналізовану практику розкриття вразливостей та секторальну мережу центрів обміну інформацією про загрози – для адаптації в Україні.

**У третьому розділі** – «*Удосконалення механізмів державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України*» – уперше розроблено концептуальну модель механізму, що інтегрує цільовий, суб'єктний, функціональний, забезпечувальний та результуючий блоки в єдиний замкнений контур управління зі зворотним зв'язком (рис. 2).

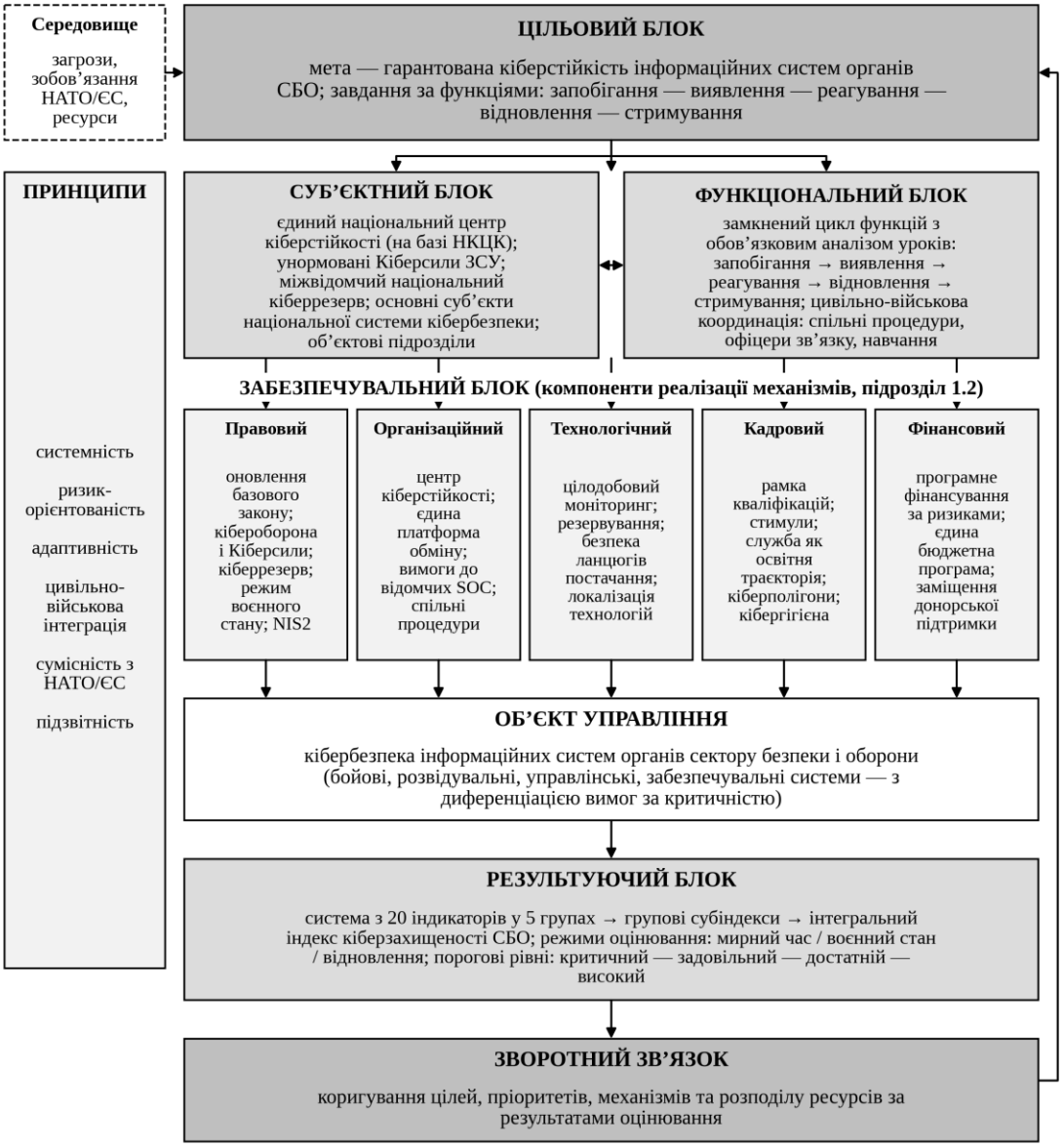



Рис. 2. Концептуальна модель механізму державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України

Цільовою категорією моделі визначено кіберстійкість. Інституційними новаціями моделі є єдиний національний центр кіберстійкості з операційними повноваженнями на базі трансформованого Національного координаційного центру кібербезпеки, унормовані Кіберсили Збройних Сил України та міжвідомчий національний кіберрезерв, який поширює передбачений законопроєктом № 12349 інститут кіберрезервістів з військового на цивільний сегмент сектору. Модель спроєктовано інваріантною до трьох сценаріїв розвитку ситуації (продовження активної фази бойових дій, стабілізація, повоєнне відновлення) та доповнено оцінкою ризиків її впровадження і запобіжників щодо них.

Обґрунтовано методологію нормування первинних показників (рис. 3) різної розмірності (кількісних, якісних та бінарних) у єдину безрозмірну шкалу та їх зваженого агрегування в інтегральний індекс кіберзахищеності сектору безпеки і оборони.

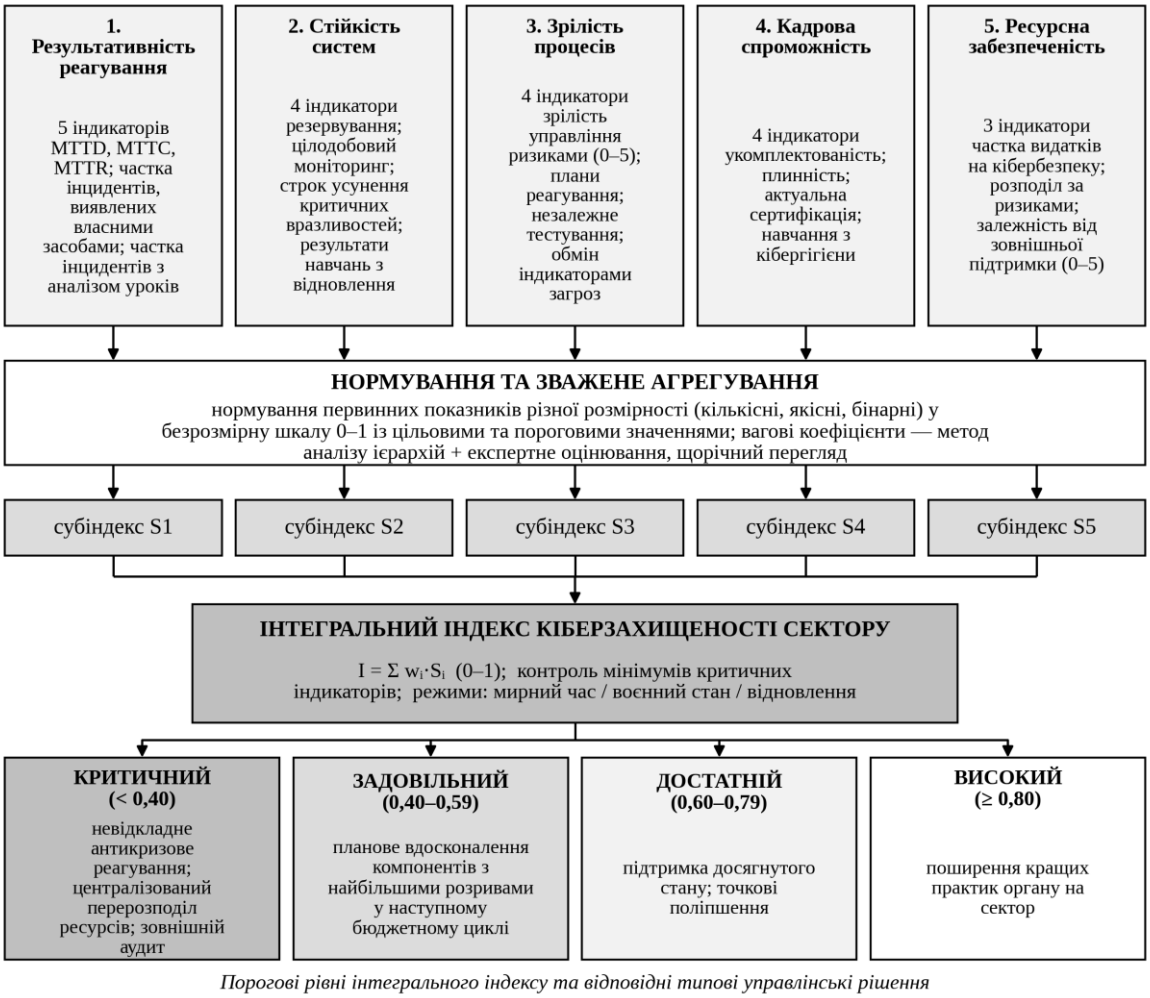



Рис. 3. Логіка агрегування індикаторів в інтегральний індекс кіберзахищеності сектору та порогові рівні управлінських рішень

Визначено чотири порогові рівні інтегрального індексу (критичний, задовільний, достатній, високий), кожному з яких відповідає типовий набір управлінських рішень – від невідкладного антикризового реагування до планового вдосконалення окремих компонентів системи, що перетворює індекс на прикладний інструмент підтримки прийняття управлінських рішень.

Сформовано комплексну систему індикаторів оцінки ефективності кіберзахисту на управлінському рівні, що охоплює двадцять базових індикаторів за п'ятьма групами (табл. 1) (результативність реагування, стійкість систем, зрілість процесів, кадрова спроможність, ресурсна забезпеченість) з методикою нормування та зваженого агрегування в інтегральний індекс кіберзахищеності сектору. Відмінними ознаками системи є секторальна специфікація, збалансованість результативних і спроможнісних вимірів та вбудованість в управлінський цикл. Порівняння з міжнародними методиками (GCI, NCSI, CMM, ENISA NCAF, NIST CSF 2.0, C2M2, оцінювання НАТО) показало, що жодна з відкритих методик не покриває рівня сектору безпеки і оборони держави, що перебуває у стані збройного конфлікту. Запропоновано триетапний порядок упровадження моделі, узгоджений з умовами воєнного часу.

Таблиця 1

Система індикаторів оцінки ефективності кіберзахисту інформаційних систем сектору безпеки і оборони на управлінському рівні (фрагмент)

| **Група** | **Базові індикатори** | **Вимір / період** |
|---|---|---|
| 1. Результативність реагування | середній час виявлення (MTTD), локалізації (MTTC) та відновлення критичних функцій (MTTR); частка інцидентів, виявлених власними засобами; частка критичних інцидентів з проведеним аналізом уроків | години; %; квартал |
| 2. Стійкість систем | частка критичних систем з актуальним резервуванням; частка систем під цілодобовим моніторингом; середній час усунення критичних вразливостей; результати навчань з відновлення | %; доби; півріччя / рік |
| 3. Зрілість процесів | рівень зрілості управління кіберризиками (0–5); частка систем з актуальними планами реагування; частка систем, що пройшли незалежне тестування; повнота обміну індикаторами загроз через єдину платформу | бали; %; квартал / рік |
| 4. Кадрова спроможність | укомплектованість посад фахівців з кібербезпеки; плинність; частка фахівців з актуальною сертифікацією; частка особового складу, що пройшла навчання з кібергігієни | %; % на рік; півріччя / рік |
| 5. Ресурсна забезпеченість | частка видатків на кібербезпеку у видатках на інформатизацію; частка видатків, розподілених за результатами оцінки ризиків; рівень залежності критичних сервісів від зовнішньої підтримки (0–5) | %; бали; рік |

Обґрунтовано механізм імплементації стандартів НАТО у сфері кібербезпеки до умов українського сектору безпеки і оборони як повторюваний п'ятиетапний цикл (рис. 4) (інвентаризація і моніторинг – пріоритезація – транспозиція – впровадження – оцінювання сумісності) з визначеним інституційним забезпеченням, середньостроковою дорожньою картою та пріоритетними сферами (захист класифікованої інформації, криптографічний захист, кібероборонні операції, реагування на інциденти, освіта і підготовка).

Визначено умови ефективної реалізації запропонованого механізму: наявність політичної волі вищого військово-політичного керівництва держави до інституційних перетворень, послідовність їх упровадження та збереження кадрового потенціалу. Обґрунтовано ризики некоректної або поспішної імплементації стандартів НАТО у сфері кібербезпеки в Україні та запропоновано управлінські заходи мінімізації цих ризиків.

Обґрунтовано, що запропоновані концептуальна модель, система індикаторів та механізм імплементації стандартів НАТО перебувають у відносинах взаємодоповнюваності: модель визначає цільову архітектуру перетворень і встановлює міжнародну сумісність як наскрізний принцип; система індикаторів забезпечує інструментарій вимірювання прогресу як щодо внутрішніх цілей моделі, так і щодо зовнішньої взаємосумісності; механізм імплементації стандартів деталізує шлях досягнення зовнішньої сумісності.

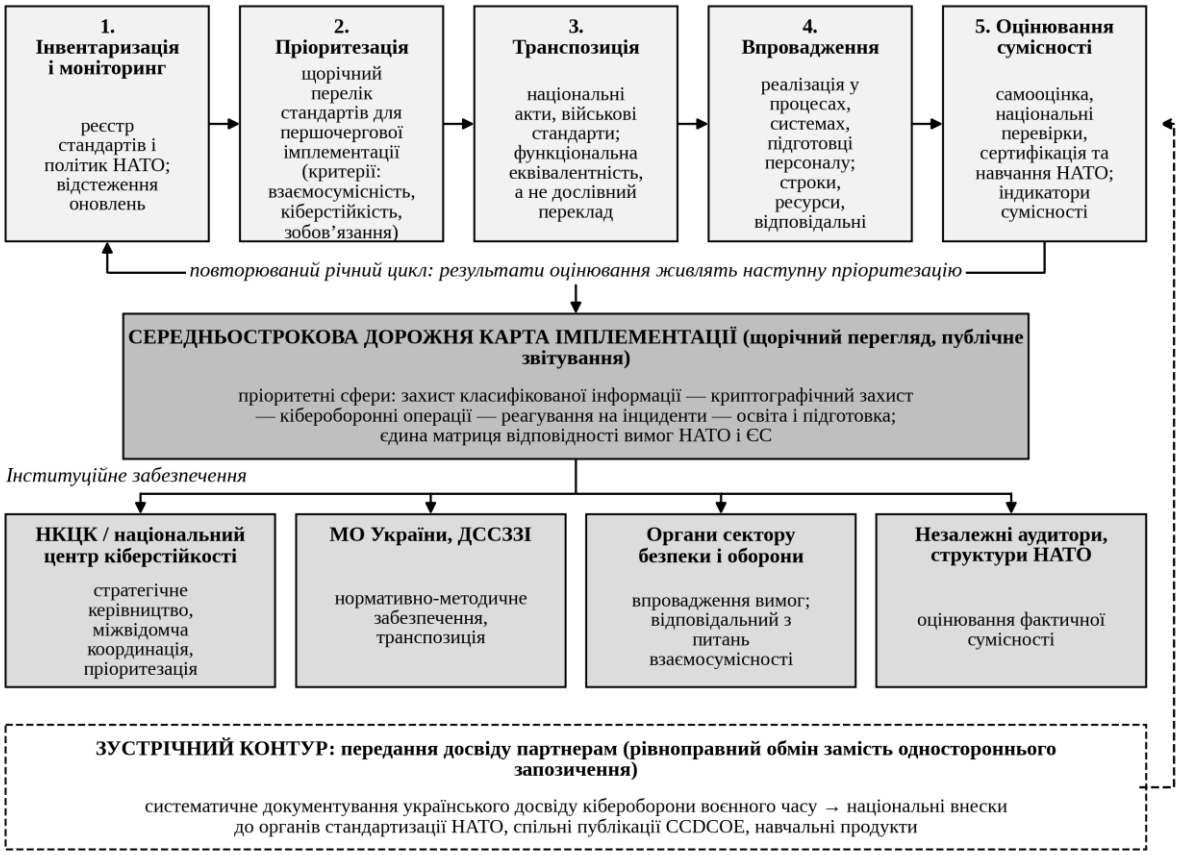



Рис. 4. Механізм імплементації стандартів НАТО у сфері кібербезпеки до умов українського сектору безпеки і оборони

Визначено очікувані ефекти впровадження запропонованого комплексу удосконалень: підвищення керованості національної системи кібербезпеки сектору безпеки і оборони, скорочення часу реагування на кіберінциденти, а також підвищення довіри партнерів по НАТО до українських структур кіберзахисту як передумови поглиблення оборонної інтеграції.

## ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та запропоновано нове вирішення актуального наукового завдання, що полягає в обґрунтуванні теоретичних засад та розробленні практичних рекомендацій щодо вдосконалення механізмів державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України. Відповідно до поставлених завдань одержано такі основні результати.

1. Досліджено теоретичні засади державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони та уточнити понятійно-категоріальний апарат у відповідній сфері. Встановлено, що поняття кібербезпеки еволюціонувало від суто технічної категорії захисту комп'ютерних систем до комплексної категорії державного управління та національної безпеки, пройшовши етапи становлення, формування, інституціоналізації та

стратегічної зрілості. Уточнено співвідношення понять «інформаційна безпека», «кібербезпека», «кіберзахист» та «захист інформації»; обґрунтовано, що стосовно інформаційних систем органів сектору безпеки і оборони кібербезпека має розглядатися у державно-управлінському вимірі – як стан захищеності, що досягається цілеспрямованим управлінським впливом уповноважених суб'єктів держави, а не лише сукупністю технічних засобів захисту. Доведено, що специфіка відповідних інформаційних систем зумовлює підвищені вимоги до механізмів державного управління їх кібербезпекою порівняно із цивільними системами. Отримані теоретичні результати створюють понятійно-методологічну основу для подальшого емпіричного аналізу, здійсненого в другому розділі дисертації, та для розроблення практико-орієнтованих рекомендацій, викладених у третьому розділі.

2. Здійснено класифікацію механізмів державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони – за природою управлінського впливу, рівнем управління та функціональним призначенням – і на цій основі систематизовано стан їх нормативно-правового забезпечення. Виокремлено п'ять етапів становлення нормативної бази кібербезпеки України та шість рівнів регулювання; виявлено системні проблеми (рамковість базового закону, термінологічну неузгодженість, дублювання повноважень, невідповідність успадкованої моделі захисту інформації технологічним реаліям, недостатню адаптованість до умов воєнного стану, незавершеність гармонізації з правом ЄС і стандартами НАТО) та обґрунтовано пріоритетні напрями вдосконалення нормативно-правової бази, зокрема системне оновлення базового законодавства із закріпленням ризик-орієнтованого підходу, законодавче унормування кібероборони та статусу кіберсил, імплементацію Директиви NIS2. Запропонована класифікація дає змогу впорядкувати розрізнені законодавчі та підзаконні акти у цілісну систему координат, придатну для подальшого моніторингу повноти нормативно-правового регулювання.

3. Проаналізовано наукові положення про інституційну систему суб'єктів державного управління кібербезпекою сектору безпеки і оборони України та механізм координації між ними. Показано, що чотирирівнева інституційна система (стратегічний, координаційний, операційний та об'єктовий рівні) є функціонально повною, однак її ефективність знижується через розмитість розмежування повноважень, множинність центрів оперативного реагування за відсутності єдиного центру управління, відомчу закритість, інституційну слабкість координаційного механізму, кадровий дефіцит та недостатню цивільно-військову інтеграцію. Встановлено, що продемонстрована в умовах безпрецедентної кібернетичної агресії стратегічна стійкість національної системи кібербезпеки значною мірою ґрунтується на надзвичайних заходах, зовнішній підтримці та неформальній взаємодії, а не на усталеній інституційній спроможності; найслабшими ланками визначено кадрове забезпечення (включно з кібергігієною особового складу, вразливість якої підтверджено аналізом кампаній 2022–2025 років проти користувачів бойових інформаційних систем),

неповноту моніторингу, фрагментацію координації реагування та відсутність системи вимірювання ефективності кіберзахисту на управлінському рівні.

4. Узагальнено підходи до адаптації зарубіжного досвіду державного управління кібербезпекою у секторі безпеки і оборони до українських реалій. На основі узагальнення досвіду США, Великої Британії, Німеччини, Франції, Польщі, Естонії, Ізраїлю, Нідерландів та інституційних платформ НАТО і ЄС виявлено стійкі закономірності ефективних національних моделей: наявність єдиного авторитетного національного органу кібербезпеки з реальними повноваженнями, інституціоналізацію військових кіберспроможностей, систематичне державно-приватне партнерство, ризик-орієнтоване управління на основі вимірюваних індикаторів, а для малих і середніх держав – волонтерські кіберрезерви та глибоку міжнародну інтеграцію. Обґрунтовано модель вибіркової адаптації, яка передбачає запозичення інституційних принципів з одночасним збереженням та інституціоналізацією унікальних українських напрацювань воєнного часу, оскільки пряме копіювання жодної із розглянутих моделей визнано недоцільним без урахування специфіки гібридної війни.

5. Розроблено концептуальну модель механізму державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України, що інтегрує цільовий, суб'єктний, функціональний, забезпечувальний та результуючий блоки в єдиний замкнений контур управління зі зворотним зв'язком, та сформовано комплексну систему індикаторів оцінки ефективності кіберзахисту на управлінському рівні. Цільовою категорією моделі визначено кіберстійкість; інституційними новаціями є єдиний національний центр кіберстійкості з операційними повноваженнями, унормовані Кіберсили Збройних Сил України та міжвідомчий національний кіберрезерв. Система індикаторів охоплює двадцять базових індикаторів за п'ятьма групами (результативність реагування, стійкість систем, зрілість процесів, кадрова спроможність, ресурсна забезпеченість) з методикою нормування та зваженого агрегування в інтегральний індекс кіберзахищеності сектору. Запропоновано триетапний порядок упровадження моделі, узгоджений з умовами воєнного часу та наявними ресурсними обмеженнями.

6. Обгрунтовано механізм імплементації стандартів НАТО у сфері кібербезпеки до умов українського сектору безпеки і оборони, який обґрунтовано як повторюваний п'ятиетапний цикл (інвентаризація і моніторинг – пріоритезація – транспозиція – впровадження – оцінювання сумісності) з визначеним інституційним забезпеченням, середньостроковою дорожньою картою та пріоритетними сферами (захист класифікованої інформації, криптографічний захист, кібероборонні операції, реагування на інциденти, освіта і підготовка). Відмінною ознакою механізму є його двосторонній характер: поряд з імплементацією стандартів Альянсу передбачено зустрічний контур систематичного документування та передання партнерам українського досвіду кібероборони воєнного часу, що перетворює процес з одностороннього запозичення на рівноправний обмін і підвищує суб'єктність України у форматі взаємодії з Альянсом.

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

*Статті у фахових виданнях*

1. Ласуков О.Є. Механізми державно-приватного партнерства у забезпеченні кібербезпеки органів сектору безпеки і оборони України. Вісник Національного університету цивільного захисту України. Серія : Державне управління. 2017. Вип. 2 (7). С. 492–501. URL: https://repositsc.nuczu.edu.ua/bitstream/123456789/29080/1/Lasukov72.pdf

2. Ласуков О.Є. Механізми міжвідомчої координації у сфері кібербезпеки сектору безпеки і оборони України: досвід воєнного стану. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2024. Вип. 1 (20). С. 461–468. https://repositsc.nuczu.edu.ua/bitstream/123456789/27744/3/Lasukov24.1.pdf

3. Lasukov O. Digital transformation of the personnel training system to ensure cybersecurity of security and defense sector agencies. Public administration and 5 state security aspects. 2024. Vol. 2. https://repositsc.nuczu.edu.ua/bitstream/123456789/27743/3/LasukovP24.2.pdf

4. Lasukov O., Esikov V. Research methods of national security as an object of public administration. Public administration and state security aspects. 2026. Vol. 1. https://repositsc.nuczu.edu.ua/bitstream/123456789/28889/1/24_Esikov.pdf

*Особистий внесок:* обґрунтовано застосування методів кейс-аналізу, SWOT-аналізу та контент-аналізу до дослідження кібербезпеки інформаційних систем органів сектору безпеки і оборони як складової національної безпеки.

5. Lasukov O. Risk-Oriented Approach in Public Administration of Cybersecurity of Information Systems of the Security and Defense Sector of Ukraine. (Ризик-орієнтований підхід у державному управлінні кібербезпекою інформаційних систем сектору безпеки і оборони України). EAST JOURNAL OF SECURITY STUDIES. Kharkiv. VOLUME 1(3)/2018. URL: https://repositsc.nuczu.edu.ua/bitstream/123456789/29077/3/Lasukov.pdf

*Наукові праці, які засвідчують апробацію матеріалів дисертації:*

6. Ласуков О., Кулаков В. Трансформація організаційно-правових механізмів безпеки в умовах воєнного стану: структурний аналіз. Теоретикопрактичні засади управління, економіки та природокористування: аспекти реінтеграції Криму в господарський комплекс України Матеріали IX Міжнародної науково-практичної конференції: 11 листопада 2025 року Київ, 2025. С. 287-290.

*Особистий внесок:* проаналізовано трансформацію нормативно-правових механізмів кібербезпеки органів сектору безпеки і оборони в умовах воєнного стану, виокремлено етапи становлення нормативної бази.

7. Ласуков О. Кіберстійкість сектору безпеки і оборони: управлінський вимір Матеріали Міжнародної науково-практичної конференції «Стратегічний розвиток держави, науки та освіти в умовах сучасних викликів» 28 серпня 2026 року м. Львів. С. 107-110.

8. Крюков О., Ласуков О. Інформаційна безпека держави в умовах глобального розвитку. Публічне управління у сфері цивільного захисту: освіта, наука, практика збірник матеріалів міжнародної науково-практичної інтернетконференції, м. Харків, 16 березня 2023 р. / за заг. ред. С.М. Домбровської. Харків : НУЦЗУ, 2023. С. 295-296.

*Особистий внесок:* уточнено співвідношення понять «інформаційна безпека», «кібербезпека», «кіберзахист» і «захист інформації» в контексті державного управління.

9. Ласуков О. Зарубіжний досвід застосування ризик-орієнтованого підходу до управління кібербезпекою у секторі оборони. Публічне управління у сфері цивільного захисту: освіта, наука, практика збірник матеріалів міжнародної науково-практичної інтернет-конференції, м. Харків, 29 березня 2024 р. м. Харків : НУЦЗУ, 2024.

## АНОТАЦІЯ

**Ласуков О. Є. Механізми державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України**. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. – Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, 2026.

Дисертацію присвячено розробленню та науковому обґрунтуванню механізмів державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України в умовах сучасних безпекових викликів. Досліджено теоретичні засади державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони, уточнено понятійно-категоріальний апарат у відповідній сфері. Класифіковано механізми державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони, а також проаналізовано стан їх нормативно-правового забезпечення, що дозволило визначити напрями його вдосконалення в умовах воєнного стану та євроатлантичної інтеграції. Проаналізовано інституційну систему суб'єктів державного управління кібербезпекою сектору безпеки і оборони й оцінено ефективність існуючих механізмів кіберзахисту інформаційних систем. Узагальнено зарубіжний досвід державного управління кібербезпекою у секторі безпеки і оборони й обґрунтовано можливості та межі його адаптації в Україні. Розроблено концептуальну модель механізму державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України. Обґрунтовано механізми імплементації стандартів НАТО у сфері кібербезпеки до умов українського сектору безпеки і оборони.

**Ключові слова:** державне управління, механізми державного управління, кібербезпека, кіберзахист, кіберстійкість, інформаційні системи, сектор безпеки і оборони, національна безпека, воєнний стан, НАТО, стандарти кібербезпеки, індикатори ефективності.

## ABSTRACT

**Lasukov O. Ye. Mechanisms of public administration of cybersecurity of information systems of the security and defence sector bodies of Ukraine**. – Qualification research paper presented as a manuscript.

Thesis for a Candidate Degree in Public Administration, speciality 25.00.02 – mechanisms of public administration. – National Aerospace University "Kharkiv Aviation Institute", Kharkiv, 2026.

The thesis is devoted to the development and scientific substantiation of mechanisms of public administration of cybersecurity of information systems of the security and defence sector bodies of Ukraine under contemporary security challenges. The subject of the research is the mechanisms of public administration of cybersecurity of information systems of the security and defence sector bodies of Ukraine.

The first chapter examines the theoretical foundations of public administration of cybersecurity: the genesis of the concept of cybersecurity is traced from a purely technical category to a comprehensive category of public administration and national security; the correlation between the concepts of information security, cybersecurity, cyber protection and information protection is clarified; the mechanisms of public administration of cybersecurity are classified by the nature of administrative influence, the level of administration and the functional purpose. The legal framework of cybersecurity of the security and defence sector bodies is analysed: five stages of its evolution are identified and systemic problems are revealed.

The second chapter analyses the current state of public administration of cybersecurity of information systems of the security and defence sector. The four-level institutional system of administration subjects is studied, and a set of coordination problems is identified. The effectiveness of the existing cyber protection mechanisms under the full-scale armed aggression is assessed; it is shown that the strategic resilience demonstrated by the national cybersecurity system is largely based on extraordinary measures, external support and informal interaction. The experience of public administration of cybersecurity of the USA, the United Kingdom, Germany, France, Poland, Estonia, Israel and the Netherlands, as well as the institutional platforms of NATO and the EU, is generalised.

The third chapter develops a set of interrelated improvements to the mechanisms of public administration of cybersecurity. For the first time, a conceptual model of the mechanism of public administration of cybersecurity of information systems of the security and defence sector bodies of Ukraine has been developed, integrating the target, subject, functional, supporting and resulting blocks into a single closed management loop with feedback. For the first time, a comprehensive system of indicators for assessing the effectiveness of cyber protection at the administrative level has been formed. A mechanism for implementing NATO cybersecurity standards has been substantiated as a repeatable five-stage cycle.

**Keywords:** public administration, mechanisms of public administration, cybersecurity, cyber protection, cyber resilience, information systems, security and defence sector, national security, martial law, NATO, cybersecurity standards, effectiveness indicators.

Відповідальний за друк *Крюков О.І.*

Підписано до друку 19.10.2026 р.
Формат 60х84 1/16. Обл.-вид. арк. 0,9.
Гарнітура Таймс. Тираж 100 прим.
Віддруковано з оригінал-макета в друкарні ФОП Леонов Д.С.
61023, м. Харків, вул. Весніна, 12, тел. (057) 717-28-80