Вікторія Чобіток[1], Тетяна Чорна[2]

АКТУАЛЬНІСТЬ ІНФОРМАЦІЙНИХ РЕСУРСІВ В СИСТЕМІ УПРАВЛІННЯ ПІДПРИЄМСТВАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА РЕГІОНАЛЬНОМУ РІВНІ

У статті представлено авторський підхід до формування регіональної системи управління інформаційними ресурсами підприємств критичної інфраструктури Харківської області в умовах воєнних загроз. Запропоновано функціональну модель, що поєднує технологічні, аналітичні, організаційні та безпекові компоненти управління даними.

Модель ґрунтується на принципах інтеграції, безперервності, кіберстійкості та взаємодії між секторами критичної інфраструктури. Її реалізація забезпечує створення єдиного регіонального інформаційного простору, підвищення ефективності управлінських рішень, зменшення наслідків кібератак і зміцнення соціально-економічної безпеки регіону.

Ключові слова: *інформаційні ресурси, критична інфраструктура, регіональна система управління, кібербезпека, цифрова трансформація, стійкість, аналітичний моніторинг, Харківська область, ситуаційний центр*

Рис. 4. Літ. 13.

DOI: 10.32752/1993-6788-2025-1-290-210-221

https://orcid.org/0000-0002-5272-388X

https://orcid.org/0000-0002-3497-2858

Viktoriia Chobitok, Tetiana Chorna

THE SIGNIFICANCE OF INFORMATION RESOURCES IN THE MANAGEMENT OF CRITICAL INFRASTRUCTURE ENTERPRISES AT THE REGIONAL LEVEL

The article presents an original approach to developing a regional information resource management system for critical infrastructure enterprises in the Kharkiv region under wartime conditions. A functional model is proposed that integrates technological, analytical, organizational, and security components of data management.

The model is based on the principles of integration, continuity, cyber resilience, and cross-sectoral interaction within critical infrastructure. Its implementation ensures the creation of a unified regional information space, enhances the effectiveness of managerial decisions, mitigates the consequences of cyberattacks, and strengthens the socio-economic security of the region.

Keywords: *information resources, critical infrastructure, regional management system, cybersecurity, digital transformation, resilience, analytical monitoring, Kharkiv region, situation center.*

Peer-reviewed, approved and placed: *13.08.2025.*

Постановка проблеми. В умовах воєнних дій та зростання кіберзагроз підприємства критичної інфраструктури стикаються з проблемою низької узгодженості інформаційних систем і відсутності єдиного центру управління даними. Розрізненість інформаційних потоків, застаріле програмне забезпечення та кадровий дефіцит у сфері IT і кіберзахисту знижують ефективність прийняття рішень та ускладнюють координацію дій між

[1] V.N. Karazin Kharkiv National University, Kharkiv. Ukraine.
[2] V.N. Karazin Kharkiv National University, Kharkiv. Ukraine.

секторами. Це призводить до затримок у реагуванні на надзвичайні ситуації й підвищує ризики втрати критичних даних.

Отже, постає проблема формування інтегрованої системи управління інформаційними ресурсами підприємств критичної інфраструктури Харківської області, здатної забезпечити безперервність, захищеність і оперативність управлінських процесів у кризових умовах.

Аналіз останніх досліджень і публікацій. Проблематика управління інформаційними ресурсами підприємств критичної інфраструктури привертає значну увагу як зарубіжних, так і вітчизняних науковців.

У працях L. Maglaras, M. Ferrag, H. Janicke та S. Kim [1] розглянуто сучасні виклики кібербезпеки критичної інфраструктури, зокрема взаємозв'язок між фізичною та інформаційною безпекою, а також підходи до побудови систем моніторингу в умовах зростання кібератак.

F. De Felice, I. Baffo та A. Petrillo [2] досліджують еволюцію управління критичними інфраструктурами в ЄС, підкреслюючи необхідність інтегрованого підходу, який об'єднує управління ризиками, цифровізацію та аналітику даних.

Питання застосування великих даних (Big Data) та штучного інтелекту у процесах оцінювання ризиків і прогнозування надзвичайних ситуацій розкрито в роботі A. Larsson та C. GroЯe [3], де акцентовано на проблемах достовірності, доступності та інтеграції інформації для забезпечення стійкості критичних об'єктів.

У вітчизняній науці дослідження сфери інформаційної безпеки критичної інфраструктури набули особливої актуальності в умовах воєнного стану.

Так, у праці В. Гаврисіва, В. Філіппової та Н. Тур [4] розглянуто аналітичні аспекти функціонування систем захисту об'єктів критичної інфраструктури, підкреслено потребу в розвитку інформаційно-аналітичних центрів для оперативного моніторингу ризиків.

О. Скіцько та Р. Ширшов [5] досліджують нормативно-правове забезпечення кібербезпеки об'єктів критичної інфраструктури, акцентуючи увагу на вдосконаленні правових механізмів та міжвідомчої взаємодії.

Окремо питання підвищення стійкості інформаційних систем у період воєнних загроз висвітлено у роботі Ю. Кірпічнікова та співавт. [6], де представлено модель оцінювання надійності інформаційної інфраструктури в умовах збройної агресії.

Метою дослідження є обґрунтування теоретичних засад і розроблення функціональної моделі регіональної системи управління інформаційними ресурсами критичної інфраструктури Харківської області, яка забезпечуватиме стійкість, інтеграцію та безпеку інформаційного середовища в умовах воєнних загроз і цифрової трансформації.

Основні результати дослідження. Інформаційні ресурси є ключовим елементом системи управління сучасними підприємствами, що забезпечують функціонування критичної інфраструктури (КІ). В умовах цифровізації економіки, воєнних загроз та підвищеної нестабільності зовнішнього середовища саме інформаційна складова визначає ефективність управлінських рішень, швидкість реагування на ризики й здатність підприємств до відновлення діяльності.

У науковій літературі інформаційні ресурси визначаються як сукупність даних, знань, документів, баз і потоків інформації, які використовуються для планування, координації та контролю управлінських процесів. У межах підприємств критичної інфраструктури (енергетичних, транспортних, комунальних, телекомунікаційних, IT-структур) інформаційні ресурси охоплюють не лише технологічну, а й економічну, аналітичну, кадрову та комунікаційну інформацію, що забезпечує прийняття рішень на різних рівнях управління [7; 13].

Інформаційні ресурси підприємств критичної інфраструктури є багаторівневою системою, що поєднує різні види даних, знань та комунікаційних потоків, необхідних для ефективного управління. Їх структура формується з урахуванням специфіки діяльності підприємств, типу об'єктів, рівня цифровізації та вимог до безпеки. Доцільно розглядати інформаційні ресурси у трьох взаємопов'язаних аспектах структурному, якісному та функціональному, що відображено на рис. 1.

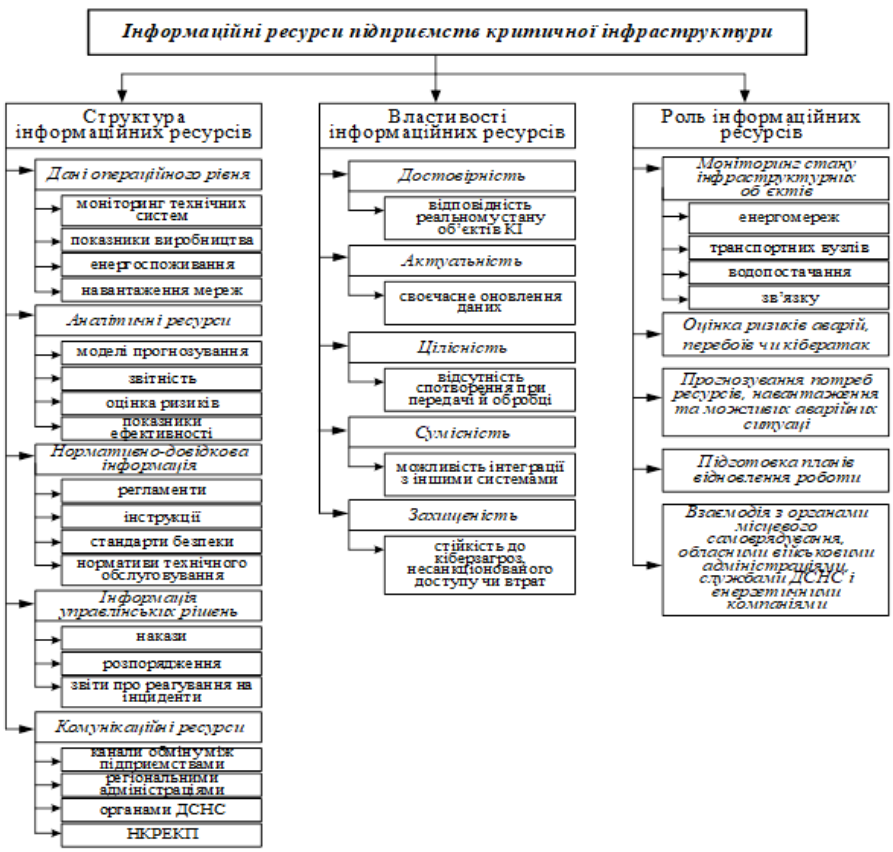

Рис. 1. **Структура, властивості та роль інформаційних ресурсів у системі управління підприємствами критичної інфраструктури,** *розроблено автором*

Як видно з рис. 1, інформаційні ресурси підприємств критичної інфраструктури утворюють цілісну систему, у якій структурні елементи, властивості та функціональні ролі тісно взаємопов'язані. Кожен компонент виконує специфічну функцію: операційні дані забезпечують базовий рівень моніторингу й контролю технічних процесів; аналітичні ресурси слугують основою для оцінки ризиків, моделювання сценаріїв і прийняття рішень; нормативно-довідкова інформація регламентує порядок дій і стандарти безпеки; інформація управлінських рішень спрямовує практичні дії персоналу; комунікаційні ресурси забезпечують координацію між усіма суб'єктами системи.

Властивості інформаційних ресурсів – достовірність, актуальність, цілісність, сумісність і захищеність – визначають їх якість та придатність до використання в управлінських процесах. Саме вони формують інформаційну стійкість підприємств критичної інфраструктури, від якої залежить точність прогнозів, швидкість реагування на ризики та ефективність управлінських рішень.

Таким чином, структурна організація та властивості інформаційних ресурсів безпосередньо впливають на їхню здатність забезпечувати управлінські рішення, підтримувати безперервність діяльності та інтегрувати підприємства критичної інфраструктури Харківської області в єдиний інформаційний простір держави.

Харківська область належить до регіонів України з високим рівнем концентрації об'єктів критичної інфраструктури, які забезпечують функціонування енергетичних, транспортних, комунальних, телекомунікаційних і інформаційно-технологічних систем. Регіон має стратегічне розташування на перетині основних логістичних коридорів Сходу та Центру країни, що зумовлює особливу важливість ефективного управління інфраструктурою в умовах підвищених ризиків.

Основу енергетичної критичної інфраструктури Харківщини становлять підприємства АТ «Харківобленерго», Харківська ТЕЦ-5, ТЕЦ-3, об'єкти «Укренерго» та локальні теплогенеруючі підприємства. Протягом 2022-2024 рр. регіон зазнав масштабних руйнувань енергетичних об'єктів унаслідок ракетних обстрілів, що призвело до зниження стійкості енергосистеми.

Управління підприємствами здійснюється переважно в режимі реактивного реагування, що зумовлено недостатньою інтеграцією інформаційних систем моніторингу. Водночас у 2023 р. «Харківобленерго» та «Теплоенерго» розпочали впровадження цифрових інструментів SCADA-типу для віддаленого контролю мереж, однак їхня взаємодія з іншими секторами (транспортом, водопостачанням, IT-комунікаціями) залишається обмеженою [8].

Харків є одним із найбільших транспортних вузлів України, через який проходять магістралі державного значення (М-03, М-18, Н-26) та залізничні коридори, що забезпечують сполучення з Полтавською, Дніпропетровською та Сумською областями.

Відновлення транспортної інфраструктури після пошкоджень ведеться активними темпами, але системи оперативного моніторингу стану доріг, мостів, руху транспорту та логістичних потоків залишаються фрагментарними.

Більшість інформаційних систем «Укравтодору» та «Укрзалізниці» не мають спільних баз даних із регіональними адміністраціями, що ускладнює прогнозування навантажень і планування ремонтних робіт [9].

Проблемним аспектом є також відсутність єдиного центру координації транспортних ризиків, який міг би оперативно обмінюватися даними з енергетичними та комунальними структурами під час надзвичайних ситуацій.

Підприємства КП «Харківводоканал», КП «Харківські теплові мережі» та місцеві житлово-експлуатаційні служби є одними з найбільш уразливих елементів регіональної КІ. Їхні інформаційні системи часто базуються на застарілому програмному забезпеченні, не мають резервних копій даних і не підключені до системи кіберзахисту.

Проблеми інформаційного забезпечення полягають у недостатньому моніторингу технічного стану мереж, несумісності баз даних і відсутності автоматизованого обліку споживання. Розрізненість інформаційних потоків призводить до втрат водних ресурсів і неефективного планування ремонтних робіт.

Харківська область має значний людський потенціал у сфері інформаційних технологій: діють десятки ІТ-компаній, технопарків і стартапів, що потенційно можуть долучитися до створення регіональної платформи управління даними. Проте цей потенціал поки використовується фрагментарно.

За оцінкою експертів Департаменту цифрової трансформації ХОВА, рівень цифрової зрілості підприємств критичної інфраструктури області у 2024 р. становив у середньому 45-50 %, що свідчить про часткове впровадження цифрових рішень без повної інтеграції даних. Найвищі показники мають енергетичні компанії, найнижчі – водопостачальні та транспортні підприємства. [10].

Виявлений аналіз діяльності підприємств критичної інфраструктури Харківської області засвідчує, що наявна система управління інформаційними потоками має низку суттєвих недоліків, які знижують ефективність прийняття управлінських рішень і створюють ризики для стабільності регіональної інфраструктури (рис. 2).

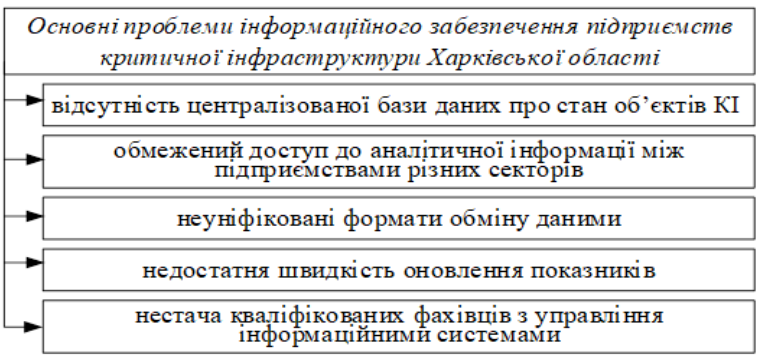

Рис. 2. **Основні проблеми інформаційного забезпечення підприємств критичної інфраструктури Харківської області,** *розроблено автором*

Як показано на рис. 2, більшість проблем пов'язана не лише з технічними аспектами, а й з організаційними обмеженнями: відсутністю інтеграції між секторами, кадровим дефіцитом і повільним оновленням інформації. У сукупності ці чинники призводять до фрагментарності управлінських процесів і знижують рівень готовності регіональної інфраструктури до кризових ситуацій.

Такі обставини підвищують вимоги до стійкості інформаційних систем, актуальності даних і рівня координації між підприємствами критичної інфраструктури, що визначає необхідність подальшого дослідження викликів і ризиків інформаційного забезпечення у регіоні.

Збройна агресія супроводжується активною фазою кібервійни, спрямованої на паралізацію інформаційних систем критичної інфраструктури. Ворожі дії поєднують фізичне ураження об'єктів із кібератаками, що створює ефект подвійного впливу – одночасне виведення з ладу технічного обладнання та інформаційних систем моніторингу. Це підтверджує, що кіберзахист є невід'ємною складовою фізичної безпеки об'єктів критичної інфраструктури, а інформаційна стійкість – важливим елементом обороноздатності регіону.

Ракетні обстріли та безпілотні атаки призводять не лише до руйнування обладнання, а й до втрати інформаційних ресурсів, розміщених на локальних серверах або в комунальних дата-центрах. Перебої з електропостачанням викликають збої у системах резервного копіювання, що створює загрозу втрати критичних технічних і управлінських даних. У таких умовах фізична загроза об'єктам критичної інфраструктури безпосередньо трансформується у загрозу інформаційній безпеці, що зумовлює потребу створення системи георезервування даних для всіх ключових підприємств регіону.

Однією з найгостріших проблем залишається відсутність інтегрованої регіональної бази даних про стан об'єктів критичної інфраструктури. Кожне підприємство - енергетичне, комунальне, транспортне чи ІТ – формує власні інформаційні системи, які не узгоджуються між собою.

У кризових умовах така роз'єднаність спричиняє затримки у прийнятті рішень, коли обласні або військові адміністрації не мають повної та оперативної картини стану інфраструктури. У періоди масованих атак на енергомережі (зокрема в грудні 2023 р. і січні 2025 р.) дані з підприємств надходили із запізненням до 6-8 годин, що унеможливлювало ефективну координацію аварійних бригад [11].

Відсутність єдиних протоколів обміну інформацією та стандартизованих форматів даних (API, XML, JSON) унеможливлює створення «цифрового ситуаційного центру» регіону, який міг би працювати в режимі реального часу.

Війна спричинила значні кадрові втрати у сфері ІТ та інформаційного менеджменту. Частина фахівців виїхала за кордон або мобілізована, що призвело до дефіциту кваліфікованих спеціалістів у державному та комунальному секторах.

Брак експертів з кіберзахисту, системного адміністрування та аналітики даних негативно впливає на здатність підприємств швидко відновлювати ІТ–інфраструктуру після атак. У ряді підприємств досі відсутні фахівці, які могли б налаштувати резервне копіювання або провести аудит кібербезпеки.

Технологічно більшість об'єктів КІ Харківщини використовують застарілі сервери та програмне забезпечення, які не підтримують сучасні стандарти безпеки. Через дефіцит фінансування закупівля нового обладнання відкладається, що підвищує ризик технічних відмов і втрати інформації.

Ще одним стратегічним викликом є розрив між обласним, муніципальним і галузевим рівнями управління даними. У результаті навіть наявна інформація використовується неефективно - дублюється або губиться на шляху передачі.

Відсутність регіонального центру управління інформаційними ресурсами призводить до того, що під час масованих атак або аварій регіональні структури змушені покладатися на ручні канали зв'язку та телефонні повідомлення. Це створює ризик втрати часу, особливо в умовах, коли оперативність рішень вимірюється хвилинами.

Інформаційна нестійкість критичної інфраструктури безпосередньо впливає на соціально-економічну стабільність Харківського регіону. Перебої в електропостачанні, водопостачанні, транспорті чи зв'язку спричиняють значні втрати бізнесу, скорочення обсягів виробництва, зниження доходів населення.

Відсутність достовірної інформації про стан мереж унеможливлює точне прогнозування економічних збитків і планування відновлювальних робіт. У 2023-2024 рр. в окремих громадах Харківщини затримка з отриманням аналітичних даних про пошкодження об'єктів призводила до подовження термінів відновлення постачання електроенергії та води до 48 годин, що мало суттєві соціальні наслідки [12-14].

Таким чином, в умовах постійних воєнних загроз система інформаційного забезпечення підприємств критичної інфраструктури Харківської області перебуває у стані високої вразливості. Вона потребує не лише технічної модернізації, а й стратегічного переосмислення - від розрізнених локальних ІТ-рішень до інтегрованої регіональної системи інформаційних ресурсів, здатної забезпечити стійке управління, безперервність діяльності та кіберфізичну безпеку в умовах війни.

Сучасні умови воєнного часу та постійні ракетні удари по об'єктах критичної інфраструктури (КІ) вимагають переходу до нової моделі управління інформаційними ресурсами, орієнтованої на швидке реагування, інтеграцію даних і забезпечення стійкості регіональної економіки. Для Харківської області, яка є одним із найуразливіших регіонів України, розвиток такої системи є не лише технічним завданням, а елементом економічної та національної безпеки.

Виявлені проблеми свідчать про необхідність побудови нової системи управління інформаційними ресурсами, яка б забезпечувала стійкість критичної інфраструктури навіть у воєнних умовах. Така система має ґрунтуватися на базових принципах, поданих на рис. 3.

Як відображено на рис. 3, запропоновані принципи формують методологічну основу для створення цілісної регіональної системи управління інформаційними ресурсами. Їх дотримання забезпечить єдність технічних стандартів, високу стійкість до зовнішніх впливів, ефективну взаємодію між

секторами критичної інфраструктури та здатність системи до адаптації у надзвичайних умовах.

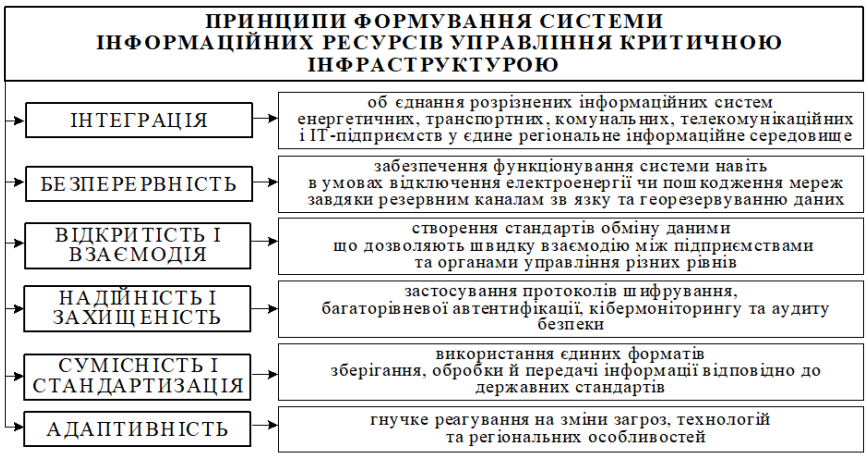

Рис. 3. **Принципи формування системи інформаційних ресурсів управління критичною інфраструктурою,** *розроблено автором*

На основі аналізу поточного стану та визначених ризиків пропонується багаторівнева модель системи інформаційних ресурсів управління КІ Харківської області (рис. 4).

Як показано на рис. 4, кожен блок системи має власні функції, інструменти реалізації та очікувані результати, які у своїй взаємодії формують цілісний контур управління інформаційними ресурсами регіону. Такий підхід дозволяє забезпечити тісний зв'язок між технологічними, аналітичними та організаційними компонентами системи, що створює основу для її ефективного функціонування та підвищення рівня стійкості критичної інфраструктури Харківської області.

Реалізація запропонованої моделі потребує створення Регіонального центру управління інформаційними ресурсами критичної інфраструктури Харківської області, який виступатиме головною координуючою ланкою системи. Центр забезпечуватиме взаємодію підприємств різних секторів, централізоване адміністрування єдиної бази даних, проведення аналітичних оцінок, підготовку звітів для обласної військової адміністрації та урядових структур. Важливим напрямом його діяльності стане підготовка й підвищення кваліфікації персоналу, а також сертифікація фахівців у сфері кіберзахисту. Центр має функціонувати у форматі цілодобового ситуаційного хабу, який акумулюватиме інформаційні потоки від енергетичних, транспортних, комунальних і телекомунікаційних підприємств, створюючи єдиний простір моніторингу, аналітики, обміну даними та оперативного реагування на надзвичайні події.

Для забезпечення ефективності функціонування така регіональна система має бути інтегрована у Національну систему захисту критичної

інфраструктури України та сумісна з провідними державними цифровими платформами.

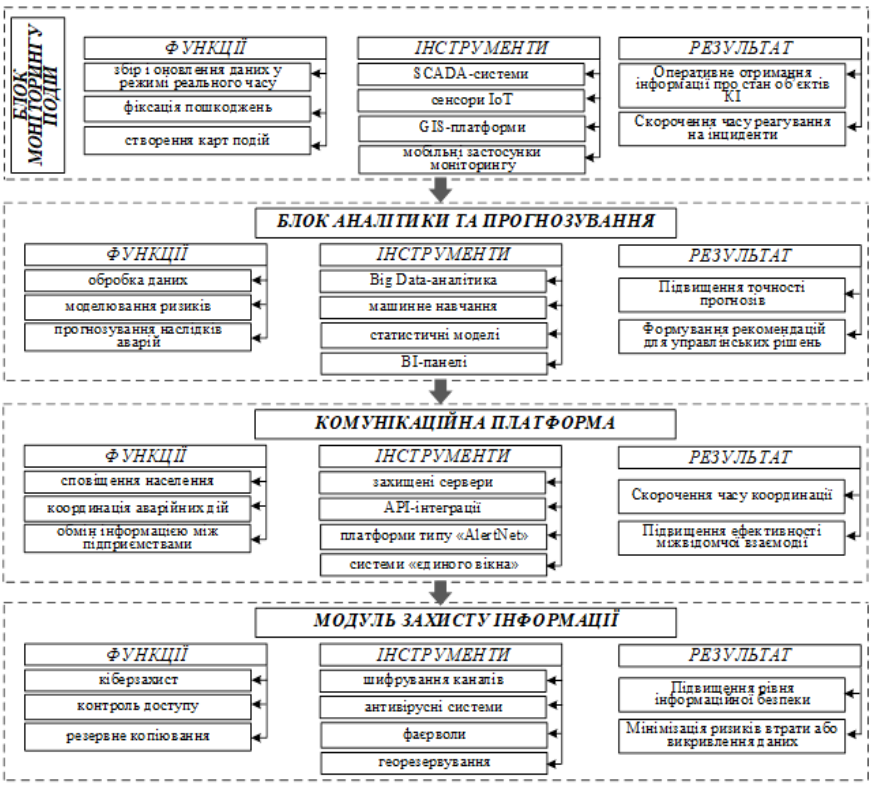

Рис. 4. **Функціональна структура, інструменти та результати регіональної системи управління інформаційними ресурсами критичної інфраструктури Харківської області,** *розроблено автором*

Зокрема, використання платформи «Дія. Цифрова держава» сприятиме оперативному обміну даними на міжрегіональному рівні, а взаємодія з Національним координаційним центром кібербезпеки при РНБО України та урядовою командою реагування на комп'ютерні надзвичайні події CERT-UA забезпечить належний рівень кіберзахисту, своєчасне реагування на кіберінциденти та підвищення загальної інформаційної безпеки підприємств критичної інфраструктури.

Така інтеграція формує єдиний інформаційний простір безпеки, у межах якого Харківська область виступатиме активним елементом загальнодержавної системи управління ризиками. Це дозволить підвищити швидкість реагування, зменшити наслідки техногенних і кібератак, зміцнити економічну та інформаційну безпеку регіону, а також посилить загальну стійкість критичної інфраструктури України.

Таким чином, розвиток системи інформаційних ресурсів управління критичною інфраструктурою Харківської області має здійснюватися за принципами інтеграції, безпеки, стійкості та взаємодії, що дозволить створити єдиний інформаційний контур регіональної безпеки, здатний ефективно функціонувати навіть в умовах військових загроз.

Висновки. Отже, інформаційні ресурси виступають системоутворювальним чинником управління підприємствами критичної інфраструктури: саме вони забезпечують достовірність і своєчасність даних, аналітичну підтримку рішень, координацію дій між секторами та безперервність операцій у воєнних умовах. Аналіз ситуації в Харківській області засвідчив високий рівень уразливості інформаційного контуру через фрагментарність систем, застарілу технічну базу, дефіцит кадрів, відсутність уніфікованих стандартів обміну і єдиного центру координації, що в умовах ракетних та кібернетичних загроз перетворюється на критичні ризики для регіональної економіки й безпеки.

Виходячи з цього, обгрунтовано необхідність переходу до цілісної регіональної системи управління інформаційними ресурсами, побудованої на принципах інтеграції, безперервності, захищеності, відкритості взаємодії, сумісності та адаптивності. Функціональна архітектура такої системи має включати узгоджені блоки моніторингу подій, аналітики та прогнозування, комунікаційної платформи і захисту інформації, а також інституційну опору у вигляді Регіонального центру управління інформаційними ресурсами.

Інтеграція регіонального рівня з національною інфраструктурою кіберстійкості, зокрема, з «Дія. Цифрова держава», Національним координаційним центром кібербезпеки при РНБО України та CERT-UA, формує єдиний інформаційний простір безпеки, підвищує швидкість реагування, зменшує наслідки техногенних і кібератак та зміцнює інформаційно-економічну стійкість Харківщини. Сукупний ефект від впорядкування інформаційних потоків, уніфікації стандартів і посилення кіберзахисту полягає у підвищенні якості управлінських рішень і створенні надійного контуру регіональної безпеки, здатного ефективно функціонувати навіть за умов тривалих воєнних загроз.

1. Maglaras L., Ferrag M., Janicke H., Kim S. Cybersecurity of Critical Infrastructures: Challenges and Solutions. Sensors. 2022. 22(14): 5105. DOI: 10.3390/s22145105

2. De Felice F., Baffo I., Petrillo A. Critical Infrastructures Overview: Past, Present and Future. Sustainability. 2022. 14(4): 2233. DOI: 10.3390/su14042233

3. Larsson A., GroЯe C. Data use and data needs in critical infrastructure risk analysis. Journal of Risk Research. 2023. P. 1–22. URL: https://doi.org/10.1080/13669877.2023.2181858

4. Гаврисів В., Філіппова В., Тур Н. Інформаційний аналіз систем захисту об'єктів критичної інфраструктури в період дії воєнного стану. Вісник ЛДУ БЖД. 2024. № 30. С. 173–187. URL: https://journal.ldubgd.edu.ua/index.php/Visnuk/article/download/2780/2666

5. Скіцько О. І., Ширшов Р. А. Нормативно-правове забезпечення кібербезпеки об'єктів критичної інфраструктури. Науковий вісник Львівського державного університету внутрішніх справ (серія юридична). 2024. № 2. С. 73–79. DOI: 10.32782/2311-8040/2024-2-11

6. Кірпічніков Ю. та ін. Модель оцінювання стійкості інформаційної інфраструктури в умовах відсічі збройної агресії. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ ім. І. Черняховського. 2025. С. 69–78.

7. Миколюк О. А., Бобровник В. М. «Особливості інформаційного забезпечення управління підприємством» – аналіз сутності інформаційного забезпечення, класифікація інформаційних ресурсів, роль інформації в управлінні. DOI: 10.31891/2307-5740-2021-294-3-7

8. Державне агентство з енергоефективності та енергозбереження України. Аналітична довідка про наслідки атак на об'єкти енергетичної інфраструктури України у 2022–2024 рр. Київ: Держенергоефективності, 2024. URL: https://saee.gov.ua/uk/news/4583

9. Міністерство розвитку громад, територій та інфраструктури України. Звіт про відновлення транспортної інфраструктури у 2022–2024 роках. Київ: Мінінфраструктури України, 2024. URL: https://mtu.gov.ua/news/34550.html

10. Департамент цифрової трансформації Харківської обласної військової адміністрації. Аналітичний звіт про стан цифрової зрілості підприємств Харківської області у 2024 році. Харків: ХОВА, 2024. URL: https://kharkivoda.gov.ua/news/121234

11. Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг (НКРЕКП). Звіт про стійкість енергетичних систем України в умовах масованих атак у грудні 2023 р. – січні 2025 р. Київ: НКРЕКП, 2025. URL: https://www.nerc.gov.ua/news/energy-resilience-report-2025

12. Харківська обласна військова адміністрація. Оперативний звіт про стан відновлення об'єктів критичної інфраструктури Харківської області у 2023–2024 роках. Харків: ХОВА, 2024.

URL: https://kharkivoda.gov.ua/news/120845

13. Чобіток В. І. Методологія наукового пізнання як основа інтелектуалізації управління холістичним розвитком підприємств. Проблеми економіки. 2020, № 1, с. 234–240. DOI: 10.32983/2222-0712-2020-1-234-240

14. Derhaliuk M., Arefieva O., Chobitok V., Kostiunik O., Shchepina T., Shostak I. (2025) Digitalization of regional economic systems in conditions of globalization challenges. Journal of Theoretical and Applied Information Technology, 2025, 28th February Vol.103. No.4 P.1503-1514.

1. Maglaras, L., Ferrag, M., Janicke, H., & Kim, S. (2022). Cybersecurity of Critical Infrastructures: Challenges and Solutions. Sensors, 22(14), 5105. https://doi.org/10.3390/s22145105

2. De Felice, F., Baffo, I., & Petrillo, A. (2022). Critical Infrastructures Overview: Past, Present and Future. Sustainability, 14(4), 2233. https://doi.org/10.3390/su14042233

3. Larsson, A., & GroЯe, C. (2023). Data Use and Data Needs in Critical Infrastructure Risk Analysis. Journal of Risk Research, 1–22. https://doi.org/10.1080/13669877.2023.2181858

4. Havrysiv, V., Filippova, V., & Tur, N. (2024). Informatsiinyi analiz system zakhystu ob'iektiv krytychnoi infrastruktury v period dii voiennoho stanu [Information Analysis of Critical Infrastructure Protection Systems during Martial Law]. Visnyk LDU BZhD, (30), 173–187. Retrieved from https://journal.ldubgd.edu.ua/index.php/Visnuk/article/download/2780/2666

5. Skitsko, O. I., & Shyrshov, R. A. (2024). Normatyvno-pravove zabezpechennia kiberbezpeky ob'iektiv krytychnoi infrastruktury [Legal Support for Cybersecurity of Critical Infrastructure Objects]. Naukovyi Visnyk Lvivskoho Derzhavnoho Universytetu Vnutrishnikh Sprav (Seriia Yurydychna), (2), 73–79. https://doi.org/10.32782/2311-8040/2024-2-11

6. Kirpichnikov, Yu., et al. (2025). Model otsiniuvannia stiikosti informatsiinoi infrastruktury v umovakh vidsichi zbroinoi ahresii [Model for Assessing the Stability of Information Infrastructure under Armed Aggression]. Zbirnyk naukovykh prats Tsentru Voienno-Stratehichnykh Doslidzhen Natsionalnoho Universytetu Oborony Ukrainy im. I. Cherniakhovskoho, 69–78.

7. Mykoliuk, O. A., & Bobrovnyk, V. M. (2021). Osoblyvosti informatsiinoho zabezpechennia upravlinnia pidpryiemstvom – analiz sutnosti informatsiinoho zabezpechennia, klasyfikatsiia informatsiinykh resursiv, rol informatsii v upravlinni [Features of Information Support for Enterprise Management]. https://doi.org/10.31891/2307-5740-2021-294-3-7

8. Derzhavne Ahentstvo z Enerhoefektyvnosti ta Enerhozberezhennia Ukrainy. (2024). Analitychna dovidka pro naslidky atak na ob'iekty enerhetychnoi infrastruktury Ukrainy u 2022–2024 rr. [Analytical Report on the Consequences of Attacks on Ukraine's Energy Infrastructure in 2022–2024]. Kyiv: Derzhenerhoefektyvnosti. Retrieved from https://saee.gov.ua/uk/news/4583

9. Ministerstvo Rozvytku Hromad, Terytorii ta Infrastruktury Ukrainy. (2024). Zvit pro vidnovlennia transportnoi infrastruktury u 2022–2024 rokakh [Report on the Restoration of Transport Infrastructure in 2022–2024]. Kyiv: Mininfrastruktury Ukrainy. Retrieved from https://mtu.gov.ua/news/34550.html

10. Departament Tsyfrovoi Transformatsii Kharkivskoi Oblasnoi Viiskovoi Administratsii. (2024). Analitychnyi zvit pro stan tsyfrovoi zrilosti pidpryiemstv Kharkivskoi oblasti u 2024 rotsi [Analytical

Report on the Digital Maturity of Enterprises in the Kharkiv Region in 2024]. Kharkiv: KhOVA. Retrieved from https://kharkivoda.gov.ua/news/121234

11. Natsionalna Komisiia, shcho zdiisniuie derzhavne rehuliuvannia u sferakh enerhetyky ta komunalnykh posluh (NKREKP). (2025). Zvit pro stiikist enerhetychnykh system Ukrainy v umovakh masovanykh atak u hrudni 2023 r. – sichni 2025 r. [Report on the Resilience of Ukraine's Energy Systems under Massive Attacks, December 2023 – January 2025]. Kyiv: NKREKP. Retrieved from https://www.nerc.gov.ua/news/energy-resilience-report-2025

12. Kharkivska Oblasna Viiskova Administratsiia. (2024). Operatyvnyi zvit pro stan vidnovlennia ob'iektiv krytychnoi infrastruktury Kharkivskoi oblasti u 2023–2024 rokakh [Operational Report on the Restoration of Critical Infrastructure Facilities of the Kharkiv Region in 2023–2024]. Kharkiv: KhOVA. Retrieved from https://kharkivoda.gov.ua/news/120845

13. Chobitok, V. I. (2020). Metodolohiia naukovoho piznannia yak osnova intelektualizatsii upravlinnia kholistychnym rozvytkom pidpryiemstv [Methodology of Scientific Cognition as the Basis for the Intellectualization of Holistic Enterprise Development Management]. Problemy Ekonomiky, (1), 234–240. https://doi.org/10.32983/2222-0712-2020-1-234-240

14. Derhaliuk M., Arefieva O., Chobitok V., Kostiunik O., Shchepina T., Shostak I. (2025) Digitalization of regional economic systems in conditions of globalization challenges. Journal of Theoretical and Applied Information Technology, 2025, 28th February Vol.103. No.4 P.1503-1514.