https://orcid.org/0000-0002-7589-2045
https://orcid.org/0000-0002-5118-1003
https://orcid.org/0000-0002-7775-6039
https://orcid.org/0000-0001-5423-0985
https://orcid.org/0000-0002-7149-4971

УДК 004.056.5:004.738.5

С.Л. РЗАЄВА[*], О.С. ЛИТВИН[*], П.М. СКЛАДАННИЙ[*,], Ю.В. КОСТЮК[*], Д.О. РЗАЄВ[***]**

МОДЕЛЬ АДАПТИВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ НА ОСНОВІ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ

[*] Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
[**] Інститут проблем математичних машин і систем НАН України, м. Київ, Україна
[***] Київський національний економічний університет імені Вадима Гетьмана, м. Київ, Україна

Анотація. *У статті розглянуто проблему управління кібербезпекою інформаційно-комунікаційних систем в умовах постійної зміни параметрів загроз, появи нових вразливостей і зростання кількості кібератак. Обґрунтовано, що традиційні статичні підходи, засновані на фіксованих політиках і наперед визначених контрзаходах, не забезпечують належного рівня захищеності під час функціонування ІКС, оскільки не враховують динаміку загрозливого середовища, трансформацію критичності активів та зміну ймовірностей реалізації загроз, що призводить до поступового накопичення ризиків. Запропоновано модель адаптивного управління кібербезпекою на основі ризик-орієнтованого підходу, яка інтегрує моніторинг подій безпеки, оцінювання локальних ризиків активів, формування інтегрального показника ризику, вибір і коригування контрзаходів та механізми зворотного зв'язку в єдиний циклічний процес. Формалізацію моделі здійснено із застосуванням функціонального моделювання IDEF0 та алгоритмічного опису. Ризик активу визначається як сума добутків імовірності реалізації релевантних загроз та потенційного збитку, що оцінюється за багатофакторною схемою з урахуванням матеріальних, функціональних і репутаційних втрат. Інтегральний показник ризику формується як зважена сума локальних ризиків з урахуванням критичності активів і встановлених порогів прийнятності. Отримані результати підтверджують зниження локальних та інтегрального ризиків і підвищення ефективності реагування системи на динамічні кіберзагрози порівняно зі статичними моделями управління безпекою.*
Ключові слова: *адаптивне управління, кібербезпека, інформаційно-комунікаційні системи, ризик-орієнтований підхід, оцінювання ризиків, інтегральний показник ризику, моделювання IDEF0.*

Abstract. *The article addresses the problem of cybersecurity management of information and communication systems under conditions of continuously changing threat parameters, the emergence of new vulnerabilities, and the growing number of cyberattacks. It is substantiated that traditional static approaches based on fixed security policies and predefined countermeasures do not ensure an adequate level of protection during the operation of information and communication systems, as they fail to consider the dynamics of the threat environment, the transformation of asset criticality, and changes in the probability of threat realization, which leads to the gradual accumulation of risks. An adaptive cybersecurity management model based on a risk-oriented approach is proposed. The model integrates security event monitoring, local asset risk assessment, formation of an integral risk indicator, selection and adjustment of countermeasures, and feedback mechanisms into a unified cyclic management process. The formalization of the model is carried out using IDEF0 functional modeling and algorithmic description. Asset risk is defined as the sum of the products of the probability of relevant threat realization and potential damage, which is assessed using a multifactor scheme taking into account material, functional, and reputational losses. The integral risk indicator is formed as a weighted sum of local risks, considering asset criticality and established acceptability thresholds. The obtained results confirm a reduction in both local and integral risks and demonstrate improved system responsiveness to dynamic cyber threats compared to static security management models.*
Keywords: *adaptive management, cybersecurity, information and communication systems, risk-oriented approach, risk assessment, integral risk indicator, IDEF0 modeling.*

ISSN 1028-9763. Математичні машини і системи. 2026. № 2

DOI: 10.34121/1028-9763-2026-2-92-109

1. Вступ

Інформаційно-комунікаційні системи (ІКС) функціонують у середовищі, яке характеризується високою динамічністю, територіально розподіленою структурою та складністю взаємодії між компонентами, що погіршує рівень кібербезпеки. Збільшення кількості та складності кібератак, активне використання багаторівневих сценаріїв експлуатації вразливостей, а також швидка еволюція загрозливого середовища формують нові виклики для систем захисту. У таких умовах традиційні підходи стають недостатніми, що обумовлює необхідність переходу до адаптивного управління ризиками, заснованого на кількісному оцінюванні загроз, формалізованому моделюванні ризиків і можливості гнучкого коригування заходів безпеки. Традиційні моделі управління безпекою, орієнтовані на застосування статичних політик і заздалегідь визначених контрзаходів, демонструють обмежену результативність у сучасному кіберпросторі. Вони не враховують змін імовірностей реалізації загроз, появу нових вразливостей та трансформацію критичності активів у часовому вимірі. Як наслідок, відбуваються поступове накопичення неврахованих ризиків і зниження ефективності систем захисту. Відсутність механізмів оперативної адаптації обмежує здатність системи своєчасно реагувати на нові виклики та приймати обґрунтовані управлінські рішення.

У зв'язку з цим впровадження адаптивних ризик-орієнтованих підходів до управління кібербезпекою ІКС, які поєднують процеси моніторингу, оцінювання ризиків, вибору контрзаходів і коригування політик безпеки в межах єдиного циклічного механізму, є актуальним. Поєднання кількісного оцінювання ризику з механізмами зворотного зв'язку забезпечує підвищення гнучкості систем захисту та їх здатності ефективно функціонувати в умовах постійних змін загрозливого середовища. У такому підході адаптивність спрямовується не лише на вдосконалення технічних засобів протидії, а й на забезпечення обґрунтованої підтримки управлінських рішень як на тактичному, так і стратегічному рівні.

Метою дослідження є розроблення моделі адаптивного управління кібербезпекою інформаційно-комунікаційних систем, заснованої на ризик-орієнтованому підході, яка передбачає формалізовану оцінку локального та інтегрального ризиків, обґрунтований вибір контрзаходів і динамічне коригування політик безпеки відповідно до змін загрозливого середовища.

Наукова новизна роботи полягає у створенні формалізованої комплексної адаптивної моделі, що інтегрує технічні, організаційні та аналітичні компоненти управління кібербезпекою в межах єдиного функціонального циклу, представленого засобами IDEF0-моделювання. У межах дослідження запропоновано використання інтегрального показника ризику як ключового критерію прийняття управлінських рішень та розроблено алгоритм функціонування моделі, який забезпечує її безперервну адаптацію до динамічних кіберзагроз. Отримані результати розширюють сучасні підходи до управління кіберризиками та формують основу для подальшого розвитку адаптивних систем кіберзахисту.

2. Аналіз сучасних досліджень і публікацій

Актуальні наукові публікації у сфері управління кібербезпекою інформаційно-комунікаційних систем засвідчують прагнення дослідників відійти від обмежених статичних моделей управління ризиками та впроваджувати більш гнучкі й адаптивні підходи. Основна увага досліджень науковців приділяється розробленню та інтеграції автоматизованих засобів моніторингу подій безпеки і реагування на кіберінциденти в ІКС. Водночас активно вдосконалюються методи оцінювання ризиків для складних і динамічних середовищ, зокрема розподілених і хмарних систем. Окремим напрямом є підвищення рівня обізнаності користувачів ІКС щодо кіберзагроз як важливої складової комплексної системи управління кібербезпекою.

Одним із внесків у цій сфері є дослідження Melaku H., у якому запропоновано контекстно-орієнтовану та адаптивну модель управління ризиками кібербезпеки [1]. У даній роботі автор критично проаналізував існуючі фреймворки управління ризиками, виявив їх переваги та обмеження, а також побудував динамічну модель, яка враховує поточні загрози та технологічні зміни в організаційному контексті. Запропоновано також набір метрик для оцінювання ефективності цієї моделі, що створює основу для об'єктивної оцінки адаптивності запропонованого підходу.

Інший напрям наукових досліджень стосується автоматизації процесів моніторингу та реагування на кіберзагрози. У статті [2] запропоновано підхід до побудови автоматизованої системи моніторингу та реагування на кіберзагрози, який базується на використанні моделі функціональних можливостей засобів кіберзахисту. Під такою моделлю автор розуміє формалізований опис функціональних можливостей засобів захисту, які забезпечують виявлення, аналіз і нейтралізацію потенційних загроз. У межах запропонованого підходу застосовуються алгоритми машинного навчання для ідентифікації аномальної поведінки та атак, що дозволяє оперативно адаптувати механізми реагування відповідно до поточного стану загрозливого середовища, забезпечуючи динамічне коригування параметрів функціонування системи безпеки.

Водночас адаптивність у сфері кібербезпеки охоплює не лише технічні аспекти реагування, а й процеси навчання та підвищення обізнаності користувачів [3–5]. Зокрема, у дослідженні [6] акцентовано увагу на питаннях оцінювання та управління ризиками інформаційної безпеки в оборонному секторі, підкреслюючи специфіку загроз у цій сфері та необхідність впровадження адаптивних організаційних і структурних рішень.

У дослідженні [7] запропоновано системну методику оцінювання та управління кіберризиками для інформаційних і керуючих систем атомних електростанцій, що поєднує кількісні та якісні підходи до аналізу загроз. Запропонований підхід передбачає класифікацію активів і джерел загроз, використання формалізованої матриці ризиків з урахуванням імовірності реалізації загрози та масштабу її впливу, а також процедуру визначення пріоритетності заходів захисту відповідно до критичності ризиків. Методика забезпечує можливість перегляду та уточнення пріоритетів захисних дій залежно від змін загрозливого середовища й експлуатаційних характеристик системи, що сприяє підвищенню результативності управління кіберризиками в об'єктах критичної інфраструктури.

Отже, аналіз наявних досліджень свідчить, що більшість із них акцентують увагу або на технічних механізмах адаптивності (моніторинг, застосування машинного навчання для виявлення аномалій, автоматизоване реагування), або на окремих організаційних аспектах (підготовка персоналу, визначення пріоритетів заходів безпеки). Водночас комплексне поєднання технічних, організаційних і аналітичних складових у межах єдиної узгодженої методики управління кіберризиками залишається недостатньо опрацьованим. Така ситуація формує наукову прогалину у частині розроблення підходів, що інтегрують кількісне оцінювання ризиків, адаптивне реагування на загрози та підтримку управлінських рішень на рівні політик безпеки. Окреслена проблема зумовлює необхідність подальших наукових досліджень, спрямованих на розроблення та формалізацію комплексних адаптивних моделей управління кібербезпекою ІКС, які забезпечують узгоджене поєднання технічних, організаційних і аналітичних засобів захисту в межах єдиного підходу.

3. Постановка задачі дослідження

У сучасних інформаційно-комунікаційних системах кіберзагрози відрізняються високою динамічністю та великою різноманітністю, що ускладнює ефективне управління безпекою. Існуючі підходи здебільшого зосереджуються на окремих складових захисту, як-от моніторинг подій безпеки, автоматизоване реагування на інциденти або навчання користувачів, і

не забезпечують комплексної інтеграції технічних, організаційних та аналітичних компонентів у єдину адаптивну методику управління ризиками. Для формалізації проблеми ІКС розглядається як об'єкт захисту, що містить апаратні та програмні компоненти, користувачів і бізнес-процеси, які взаємодіють між собою та можуть піддаватися різним кіберзагрозам. У межах цього підходу визначаються ключові множини.

Активи (A) — ресурси системи, що потребують захисту (дані, сервери, мережеві компоненти, критичні процеси тощо).

Загрози (T) — події або дії, здатні завдати шкоди активам (кібератаки, технічні збої, помилки користувачів).

Вразливості (V) — слабкі місця активів або процесів, які можуть бути використані загрозами.

Контрзаходи (C) — технічні, організаційні та процедурні засоби захисту, що знижують імовірність реалізації загроз і мінімізують наслідки інцидентів.

На основі цієї формалізації наукова задача дослідження полягає у розробці адаптивного ризик-орієнтованого підходу до управління кібербезпекою ІКС, який забезпечує:

• кількісну оцінку ризиків для кожного активу, що включає ймовірність реалізації конкретних загроз (кібератак, технічних збоїв, людських помилок тощо) та потенційний збиток у разі їх реалізації;

• формування інтегрального показника ризику, який поєднує ймовірність загрози та величину можливого збитку для окремих активів у загальну оцінку стану безпеки системи;

• підтримку прийняття управлінських рішень, зокрема визначення оптимальних контрзаходів та їх пріоритетів, виходячи з інтегрального рівня ризику;

• динамічну адаптацію політик безпеки з метою коригування пріоритетів та заходів захисту відповідно до змін загрозливого середовища і стану ІКС у реальному часі.

Вхідними параметрами моделі є: конфігурація активів A, множини загроз T, вразливості V, стан системи безпеки та зовнішні фактори впливу.

Вихідними параметрами моделі є:

• оптимальний набір контрзаходів C^* для кожного активу;

• кількісна оцінка ризиків активів, що включає ймовірність реалізації загроз та потенційний збиток;

• інтегральний показник ризику, що відображає загальний стан безпеки ІКС;

• рекомендації щодо пріоритетів управлінських рішень, сформовані на основі інтегрального ризику та оцінки ефективності контрзаходів.

Досягнення поставленої задачі дозволяє перейти до ризик-орієнтованого підходу, який базується на кількісній оцінці загроз і потенційного збитку для активів ІКС, формуванні інтегрального показника ризику та визначенні критеріїв управлінських рішень.

4. Мета і задачі дослідження

Метою дослідження є розроблення формалізованої моделі адаптивного управління кібербезпекою інформаційно-комунікаційних систем на основі ризик-орієнтованого підходу, яка забезпечує безперервний цикл «моніторинг — оцінювання ризиків — вибір і коригування контрзаходів — оновлення політик — зворотний зв'язок» та дає змогу підтримувати локальні й інтегральний ризики на рівні нижче встановлених порогів у динамічному загрозливому середовищі.

Для досягнення цієї мети виконуються такі взаємопов'язані задачі: аналізуються обмеження статичних підходів управління безпекою та обґрунтовується потреба адаптивного керування; формалізуються ключові множини активів, загроз, вразливостей і контрзаходів та визначаються вхідні й вихідні параметри моделі; розробляється математичний апарат кількісного оцінювання локального ризику активу як функції ймовірності реалізації загроз і

потенційного збитку, а також формується інтегральний показник ризику з урахуванням критичності активів; встановлюються порогові значення прийнятності ризику та правила переходу між режимами функціонування системи; будується функціональна структура моделі засобами IDEF0 з визначенням входів, керуючих впливів, механізмів і виходів кожного модуля; розробляється алгоритм роботи моделі у вигляді чіткої послідовності кроків і псевдокоду; здійснюється оцінювання ефективності моделі шляхом порівняння локальних та інтегрального ризиків до і після застосування адаптивних механізмів і обґрунтовуються переваги запропонованого підходу порівняно зі статичними моделями; додатково визначаються обмеження та напрями подальшого розвитку, зокрема щодо автоматизації налаштування параметрів ризику, інтеграції методів машинного навчання та адаптації до розподілених і хмарних середовищ.

5. Основні положення ризик-орієнтованого підходу

Ризик-орієнтований підхід до управління кібербезпекою ІКС передбачає системну оцінку та керування ризиками на основі кількісних і якісних характеристик загроз та активів. Ризик кібербезпеки для окремого активу $a_i \in A$ визначається як комбінація ймовірності реалізації загрози та потенційного збитку, який може бути завданий активу, і розраховується за формулою

$$R(a_i) = \sum_{t_j \in T_i} P(t_j) \cdot L(a_i, t_j), \quad (1)$$

де $R(a_i)$ — ризик для активу a_i, $T_i \subseteq T$ — множина загроз, що впливають на актив, $P(t_j)$ — ймовірність реалізації t_jзагрози, $L(a_i, t_j)$ — потенційний збиток. Імовірність $P(t_j)$ визначається з урахуванням історичних даних, аналітики подій безпеки, виявлених вразливостей та ефективності застосованих контрзаходів і є динамічним параметром, що змінюється у залежності від стану системи та загрозливого середовища. Потенційний збиток $L(a_i, t_j)$, завданий активу a_i унаслідок реалізації загрози t_j, оцінюється з використанням багатофакторного підходу з урахуванням матеріальних, функціональних та репутаційних втрат.

$$L(a_i, t_j) = \propto \cdot\ L_{mat}(a_i, t_j) + \beta \cdot L_{func}(a_i, t_j) + \gamma \cdot L_{rep}(a_i, t_j), \quad (2)$$

де $L_{mat}(a_i, t_j)$ — матеріальні втрати активу, $L_{func}(a_i, t_j)$ — втрати, пов'язані з порушенням функціонування інформаційно-комунікаційної системи, $L_{rep}(a_i, t_j)$ — репутаційні втрати, обумовлені реалізацією відповідної загрози, α, β, γ — коефіцієнти вагомості кожного виду збитку та встановлюються експертним шляхом або відповідно до внутрішніх політик інформаційної безпеки організації.

Для оцінки загального рівня ризику ІКС застосовується інтегральний показник, який дозволяє оцінювати ефективність комплексних заходів безпеки та порівнювати різні сценарії захисту:

$$R_{int} = \sum_{i=1}^{n} w_i \cdot R(a_i), \quad (3)$$

де w_i — коефіцієнт критичності активу a_i, що відображає його значущість для функціонування системи.

Для інтегрального ризику системи вводиться порогове значення $R^{int}_{thresholdint}$, яке визначає гранично допустимий рівень сукупного ризику. Якщо $R_{int} \le R^{int}_{thresholdint}$, стан безпеки інформаційно-комунікаційної системи вважається допустимим і не потребує впровадження додаткових контрзаходів, окрім підтримувальних та регламентних заходів безпеки. У разі,

якщо $R_{int} > R^{int}_{thresholdint}$, рівень ризику оцінюється як неприйнятний, що зумовлює необхідність застосування додаткових контрзаходів або посилення наявних механізмів захисту.

Аналогічно для оцінювання ризику окремих активів використовується порогове значення $R^{local}_{thresholdint}$. Якщо для активу a_i виконується умова $R(a_i) \le R^{local}_{thresholdint}$, рівень ризику вважається допустимим, і заходи безпеки щодо цього активу обмежуються підтриманням поточного рівня захисту. Якщо ж $R(a_i) > R^{local}_{thresholdint}$, ризик вважається неприйнятним, а це, насамперед, свідчить про необхідність коригування або посилення заходів безпеки для відповідного активу незалежно від значення інтегрального ризику системи.

Пріоритетність контрзаходів визначається на основі їхнього впливу на зменшення інтегрального ризику та ефективності використання ресурсів, а адаптивне коригування політик безпеки здійснюється в режимі реального часу у відповідь на зміни загрозливого середовища, появу нових вразливостей або зміну критичності активів. Ризик-орієнтований підхід дозволяє забезпечити комплексну інтеграцію технічних і організаційних заходів захисту, оперативно реагувати на динамічні загрози, кількісно оцінювати ефективність контрзаходів, створивши при цьому основу для розвитку формалізованих алгоритмів адаптивного управління кібербезпекою.

6. Модель адаптивного управління кібербезпекою

Модель адаптивного управління кібербезпекою інформаційно-комунікаційних систем передбачає постійне поєднання процесів моніторингу, оцінки ризиків, підбору заходів захисту та аналізу зворотного зв'язку в єдиний циклічний процес. Це дозволяє підтримувати безпеку на прийнятному рівні в режимі реального часу. Концептуально модель базується на принципі «спостереження — оцінка — реагування — коригування», що дає змогу динамічно змінювати політики безпеки та пріоритети контрзаходів залежно від результатів оцінки ризиків, змін у загрозливому середовищі, появи нових вразливостей або зміни важливості активів.

Для наочності та структурованого представлення складних процесів модель зображено у вигляді IDEF0-діаграми, яка дозволяє чітко показати функціональні блоки, їхні входи та виходи, керуючі впливи та механізми реалізації. На верхньому рівні моделі виділено чотири основні компоненти: моніторинг подій безпеки, оцінка ризиків, вибір і коригування заходів захисту, а також зворотний зв'язок і навчання системи (рис. 1).

Компонент моделі «Моніторинг подій безпеки» містить збір даних про інциденти, аномалії та підозрілі дії, використання логів, систем управління подіями безпеки (SIEM) та алгоритмів машинного навчання для виявлення нових загроз. На основі отриманої інформації формується актуальна оцінка стану ІКС, яка стає вхідною для блоку оцінювання ризиків.

Компонент моделі «Оцінювання ризиків» реалізує кількісну та якісну оцінки загроз, враховуючи ймовірність їх реалізації, потенційний збиток для активів та взаємозв'язки між компонентами ІКС. Результатом цього етапу є інтегральний показник ризику, який служить критерієм для прийняття рішень щодо заходів захисту.

Компонент моделі «Вибір та коригування контрзаходів» функціонує на основі результатів оцінювання локального та інтегрального показників ризику з урахуванням відповідних порогових значень допустимого ризику. У межах даного компонента система формує оптимальний набір контрзаходів для кожного активу та визначає пріоритетність їх застосування з урахуванням очікуваного ефекту зниження ризику, ресурсних обмежень і чинних політик безпеки. Коригування контрзаходів здійснюється в адаптивному режимі у відповідь на зміну параметрів загроз, появу нових вразливостей або зміну критичності активів інфор-

маційно-комунікаційної системи. Отже, запропонована модель забезпечує інтегроване поєднання аналітичних, технічних та організаційних механізмів кіберзахисту в межах замкненого адаптивного циклу управління.

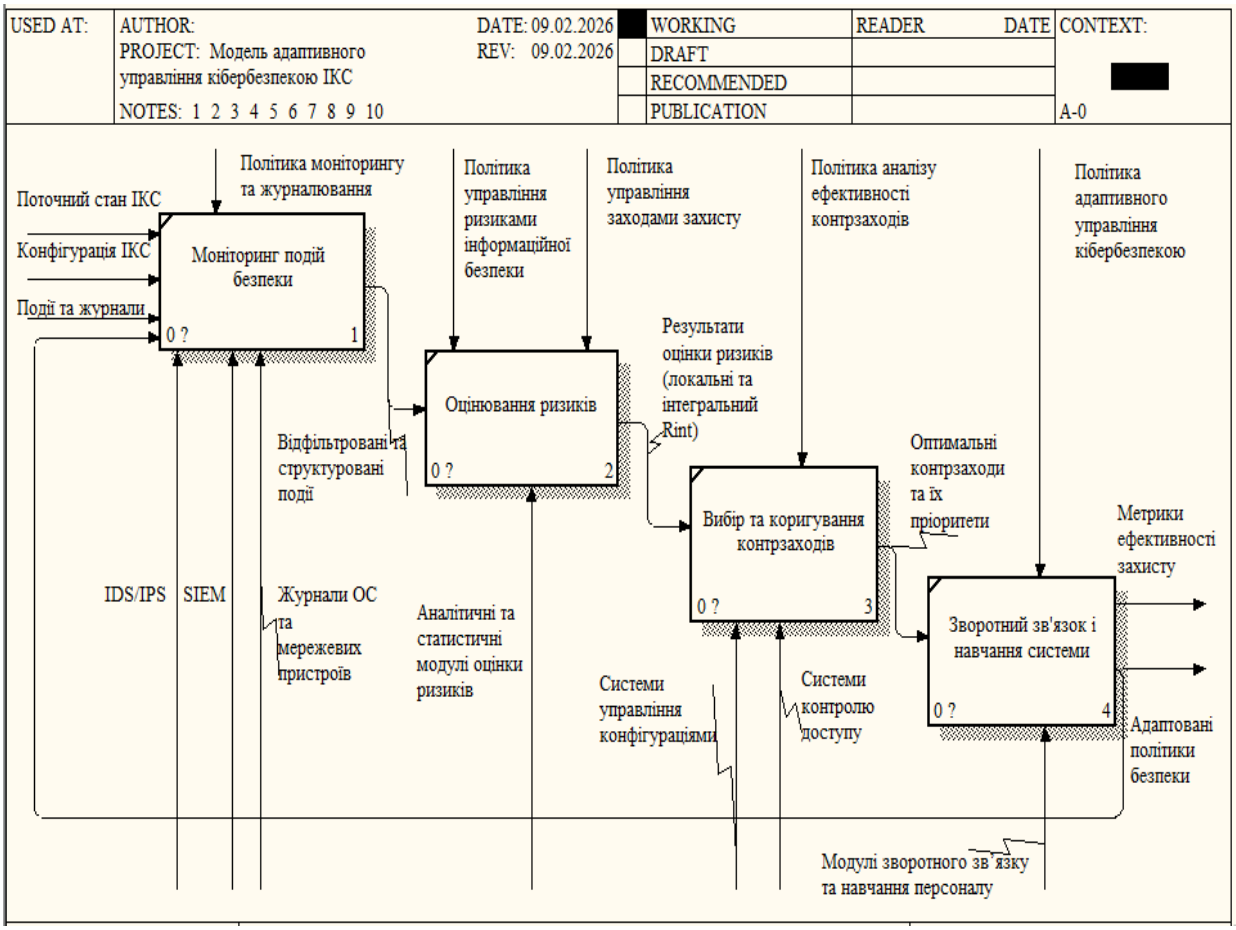

Рисунок 1 — Модель адаптивного управління кібербезпекою інформаційно-комунікаційних систем

Компонент моделі «Зворотний зв’язок і навчання системи» забезпечує адаптивність моделі, де аналізується та оцінюється ефективність впроваджених контрзаходів, оновлюються політики безпеки та правила поведінки користувачів, а також враховуються дані про нові загрози. Тобто даний підхід дозволяє системі самостійно навчатися, підвищувати точність оцінки ризиків і зменшувати залежність безпеки від людського фактора.

У розробленій моделі адаптивного управління кібербезпекою інформаційно-комунікаційних систем використано функціональне моделювання IDEF0. Вхідні стрілки моделі представляють інформаційні потоки, що надходять до кожного функціонального блоку, і забезпечують необхідні дані для оцінки стану системи, аналізу ризиків, вибору контрзаходів та коригування політик безпеки. Стрілки керування відображають нормативні, організаційні та політичні обмеження, які визначають правила функціонування кожного блоку моделі та встановлюють критерії прийняття рішень. Стрілки механізмів і виходів передусім демонструють технічні засоби реалізації процесів та результати їх виконання, що формують основу для наступного циклу адаптивного управління.

У табл. 1 наведено узагальнену інформацію щодо значення цих вхідних стрілок, їх зміст та роль у роботі моделі.

Таблиця 1 — Вхідні стрілки моделі адаптивного управління кібербезпекою ІКС

Модуль моделі	Назва вхідної стрілки	Зміст вхідної інформації	Роль у моделі
Моніторинг подій безпеки	Поточний стан ІКС	Дані про поточне функціонування апаратних і програмних компонентів, стан мережевих з'єднань, активність користувачів та сервісів	Забезпечує контекстну основу для коректної інтерпретації подій безпеки та виявлення відхилень від нормального режиму роботи
	Конфігурація ІКС	Опис архітектури ІКС, склад і параметри компонентів, логічні та фізичні взаємозв'язки між активами	Дозволяє ідентифікувати, до яких активів належать зафіксовані події, та оцінити їхню потенційну критичність
	Події та журнали	Журнали доступу, мережевий трафік, системні повідомлення, записи про помилки, спроби несанкціонованого доступу	Джерело даних для виявлення, класифікації та кореляції подій безпеки, включаючи інциденти, аномалії та підозрілі дії
	Адаптовані політики безпеки	Актуалізовані правила, налаштування та обмеження безпеки, сформовані на основі результатів попередніх циклів управління моделлю	Визначають умови, правила та пороги виявлення подій безпеки, а також впливають на параметри збору, фільтрації та аналізу інформації
Оцінювання ризиків	Відфільтровані та структуровані події	Результати кореляції та аналізу подій, отримані з модуля моніторингу, з прив'язкою до активів та типів загроз	Використовуються як вхідні дані для розрахунку ймовірностей реалізації загроз та формування локального й інтегрального показників ризику
Вибір та коригування контрзаходів	Результати оцінювання ризиків	Значення локальних ризиків для окремих активів та інтегрального ризику ІКС, отримані в модулі оцінювання ризиків	Формують основу для прийняття управлінських рішень щодо вибору, пріоритезації та коригування контрзаходів
Зворотний зв'язок і навчання системи	Обрані контрзаходи та їх пріоритети	Інформація про застосовані контрзаходи, рівень їхньої пріоритетності та очікуваний вплив на зниження ризиків	Використовується для оцінки ефективності реалізованих заходів, оновлення параметрів моделі та адаптації політик безпеки

У моделі адаптивного управління кібербезпекою ІКС стрілки контролю визначають нормативні та організаційні обмеження функціонування моделі. Вони відображають політики, стандарти та правила, що регламентують процеси моніторингу, оцінювання ризиків, вибору контрзаходів і адаптації політик безпеки.

У табл. 2 наведено узагальнений опис стрілок контролю моделі з посиланням на відповідну нормативну базу та зміст політик безпеки.

Таблиця 2 — Стрілки контролю моделі адаптивного управління кібербезпекою ІКС

Модуль моделі	Назва стрілки контролю	Нормативна база	Опис політики
Моніторинг подій безпеки	Політика моніторингу та реєстрації подій	ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-92	Визначає правила збору, кореляції, зберігання та аналізу подій безпеки, вимоги до журналювання, часової синхронізації та реагування на аномалії в ІКС
Оцінювання ризиків	Політика управління ризиками інформаційної безпеки	ISO/IEC 27005, ISO 31000, NIST SP 800-30	Встановлює методи і критерії оцінювання ймовірності загроз, потенційного збитку та визначення інтегрального показника ризику для активів ІКС
	Політика управління заходами захисту	ISO/IEC 27002, NIST SP 800-53	Регламентує вибір, впровадження та пріоритезацію технічних і організаційних контрзаходів залежно від рівня ризику та критичності активів
Вибір та коригування контрзаходів	Політика аналізу ефективності контрзаходів	ISO/IEC 27004, NIST SP 800-55	Встановлює метрики та показники ефективності заходів безпеки, порядок збору та аналізу результатів для коригування політик і процедур
Зворотний зв’язок і навчання системи	Політика адаптивного управління кібербезпекою	ISO/IEC 27001, ISO/IEC 27005, NIST CSF	Визначає механізми коригування політик безпеки на основі зворотного зв’язку, результатів оцінювання ризиків та змін загрозливого середовища

У моделі адаптивного управління кібербезпекою ІКС стрілки механізмів визначають технічні та організаційні засоби, які реалізують функції кожного блоку, що містять програмні рішення, апаратні пристрої, методи обробки даних та модулі навчання персоналу, з метою забезпечення ефективного виконання компонентів моделі (табл. 3).

Таблиця 3 — Механізми моделі адаптивного управління кібербезпекою ІКС

Модуль моделі	Назва механізму	Зміст / склад механізму	Роль у моделі
Моніторинг подій безпеки	SIEM	Система управління інформацією та подіями безпеки, збір, кореляція та аналіз логів	Забезпечує централізований моніторинг подій та виявлення аномалій
	IDS/IPS	Системи виявлення та запобігання вторгнень у мережу	Виявлення підозрілих активностей та блокування загроз у реальному часі

Продовж. табл. 3

	Журнали мережевих та системних пристроїв	Логи серверів, мережевих комутаторів, кінцевих пристроїв	Джерело інформації про події безпеки з метою подальшої її оцінки
Оцінювання ризиків	Аналітичні модулі оцінки ризиків	Програмні та статистичні інструменти для розрахунку ймовірності загроз та потенційних збитків	Забезпечує кількісне та якісне оцінювання локальних та інтегральних ризиків
Вибір та коригування контрзаходів	Системи управління конфігурацією	Інструменти управління налаштуваннями компонентів ІКС	Дозволяють реалізувати технічні контрзаходи відповідно до політик безпеки
	Системи контролю доступу	Механізми управління правами користувачів та ролями	Забезпечують виконання політик доступу і мінімізацію ризиків несанкціонованого доступу
Зворотний зв’язок і навчання системи	Модулі зворотного зв’язку	Програмні засоби збору даних про ефективність контрзаходів та стан активів після впровадження відповідних контрзаходів	Дозволяють відстежувати результати впроваджених контрзаходів і формувати дані для адаптації
	Модулі навчання персоналу	Інтерактивні платформи, тренажери та симулятори кіберінцидентів	Підвищують обізнаність персоналу й адаптивність політик безпеки

Вихідні стрілки моделі адаптивного управління кібербезпекою ІКС відображають результати виконання функціональних блоків та забезпечують передачу сформованих рішень, показників і рекомендацій між етапами управління (табл. 4). Вони характеризують рівень ризику, обрані контрзаходи, метрики ефективності та адаптовані політики безпеки, що формують підґрунтя для подальшого циклу управління.

Таблиця 4 — Вихідні стрілки моделі адаптивного управління кібербезпекою ІКС

Модуль моделі	Назва вихідної стрілки	Зміст вихідної інформації	Роль у моделі
Моніторинг подій безпеки	Відфільтровані та структуровані події	Нормалізовані, корельовані та класифіковані події безпеки	Забезпечує підготовку даних для подальшого оцінювання ризиків
Оцінювання ризиків	Результати оцінки ризиків	Локальні ризики для окремих активів та інтегральний показник ризику (R_{int})	Формує кількісну та якісну основи для прийняття управлінських рішень
Вибір та коригування контрзаходів	Оптимальні контрзаходи та їх пріоритети	Перелік технічних і організаційних заходів захисту з визначеними пріоритетами	Забезпечує цілеспрямоване зниження рівня ризику

Продовж. табл. 4

Зворотний зв'язок і навчання системи	Метрики ефективності захисту	Показники результативності контрзаходів і рівня безпеки	Дає змогу оцінити ефективність реалізованих рішень
	Адаптовані політики безпеки	Оновлені правила, пріоритети та параметри політик безпеки	Забезпечує адаптацію системи до змін загрозливого середовища та стану ІКС

Розроблена модель адаптивного управління кібербезпекою інформаційно-комунікаційних систем реалізує поставлену задачу дослідження. ІКС формалізовано як об'єкт захисту з множинами активів, загроз, вразливостей і контрзаходів, які представлені у вигляді вхідних інформаційних потоків, функціональних модулів і вихідних результатів IDEF0-моделі. Модуль моніторингу оновлює дані про загрози та стан системи, модуль оцінювання ризиків проводить кількісну та якісну оцінки ризиків і формує інтегральний показник ризику та оцінку локальних ризиків активів, модуль вибору контрзаходів підтримує прийняття управлінських рішень, а механізм зворотного зв'язку забезпечує динамічну адаптацію політик безпеки. Отже, модель є інструментом практичного впровадження ризик-орієнтованого підходу до управління кібербезпекою й інтегрує аналітичні, технічні та управлінські процеси в єдиний адаптивний цикл, що дозволяє досягати цілей даного дослідження.

Запропонована структура моделі забезпечує формалізований зв'язок між кількісною оцінкою ризиків і практичними управлінськими рішеннями, що підвищує прозорість та обґрунтованість процесу управління кібербезпекою. Її застосування створює методичну основу для побудови автоматизованих систем підтримки прийняття рішень у сфері кіберзахисту та забезпечує масштабованість підходу для інформаційно-комунікаційних систем різного рівня складності.

7. Алгоритм функціонування моделі адаптивного управління

Алгоритм реалізації адаптивного управління кібербезпекою інформаційно-комунікаційних систем базується на циклічній ризик-орієнтованій взаємодії чотирьох функціональних модулів та забезпечує динамічну адаптацію політик безпеки відповідно до змін загрозливого середовища та стану ІКС (рис. 2).

Крок 1. Моніторинг подій безпеки та стану ІКС

Функціонування алгоритму адаптивного управління кібербезпекою починається з постійного моніторингу подій безпеки та поточного стану інформаційно-комунікаційної системи. На цьому етапі відбувається збір телеметричних даних із журналів доступу, мережевого трафіку, системних логів, а також сигналів від SIEM і IDS/IPS. Зібрана інформація аналізується з урахуванням конфігурації системи та структури її активів, що дозволяє коректно інтерпретувати події та виявляти відхилення від нормальної роботи.

Крок 2. Фільтрація, нормалізація та структуризація подій

На другому етапі проводиться первинна обробка зібраних даних щодо подій, а саме: видалення шумових даних, приведення подій до єдиного формату та сортування за типами загроз. Кожна подія зв'язується з відповідним активом a_i, виявленими вразливостями та можливими сценаріями атак. У результаті формується структурований набір подій, який підходить для подальшого якісного та кількісного аналізу ризиків.

Крок 3. Оцінювання локальних ризиків активів

На основі структурованих подій, у модулі оцінювання, здійснюється розрахунок ризику для кожного активу $a_i \in A$. Ризик визначається як сума добутків імовірностей реалізації відповідних загроз та потенційного збитку, які вони можуть завдати активу, розрахованого за формулою (1). Ймовірність реалізації загрози $P(t_j)$ є динамічним параметром і коригується з урахуванням інтенсивності подій безпеки, наявних вразливостей та ефективності вже застосованих контрзаходів. Потенційний збиток $L(a_i, t_j)$ оцінюється багатофакторно, що дозволяє врахувати матеріальні, функціональні та репутаційні втрати.

Крок 4. Формування інтегрального показника ризику ІКС

Після оцінювання локальних ризиків активів здійснюється їх агрегування з урахуванням коефіцієнтів критичності активів w_i. Інтегральний показник ризику ІКС визначається за формулою (3). Отримане значення характеризує загальний стан кібербезпеки ІКС та використовується як узагальнений критерій для прийняття управлінських рішень.

Крок 5. Аналіз прийнятності рівня ризику

На цьому етапі інтегральний показник ризику системи R_{int} порівнюється з пороговим значенням допустимого інтегрального ризику $R^{int}_{thresholdint}$, визначеним політиками інформаційної безпеки. Якщо виконується умова $R_{int} \le R^{int}_{thresholdint}$, стан безпеки системи вважається допустимим, і система продовжує функціонування в режимі моніторингу та уточнення параметрів моделі. У разі, якщо $R_{int} > R^{int}_{thresholdint}$, рівень ризику оцінюється як неприйнятний, що ініціює перехід алгоритму до режиму активного адаптивного реагування. Паралельно для кожного активу a_i оцінюється локальний ризик $R(a_i)$ і порівнюється з порогом $R^{local}_{thresholdint}$. Якщо $(a_i) \le R^{local}_{thresholdint}$, ризик активу вважається допустимим, і заходи безпеки обмежуються підтриманням поточного рівня захисту. Якщо ж $R(a_i) > R^{local}_{thresholdint}$, ризик активу оцінюється як неприйнятний, що зумовлює необхідність застосування додаткових контрзаходів або посилення наявних механізмів захисту для цього активу незалежно від інтегрального ризику системи.

Крок 6. Вибір і коригування контрзаходів

Якщо рівень ризику перевищує встановлені порогові значення, складається перелік можливих контрзаходів для тих активів, які потребують додаткового захисту. Кожен контрзахід оцінюється з точки зору того, наскільки він знижує локальний та інтегральний показники ризику. Далі визначається їх пріоритетність, враховуючи наявні ресурси, поточний стан системи та чинні політики безпеки.

Крок 7. Реалізація контрзаходів та оновлення політик безпеки

Визначені контрзаходи впроваджуються в систему, що може включати зміну прав доступу, посилення механізмів контролю, оновлення програмного забезпечення або застосування організаційних заходів. Одночасно оновлюються політики безпеки, щоб вони відображали нові пріоритети захисту активів та результати оцінки ризиків.

Крок 8. Формування зворотного зв'язку та ініціація нового циклу

На завершальному етапі оцінюється ефективність реалізованих контрзаходів, уточнюються параметри оцінювання ризиків і оновлюється база знань системи. Отримані результати використовуються для початку нового циклу моніторингу, забезпечуючи безперервне адаптивне управління безпекою.

Умови переходу між станами системи

Перехід між станами системи в алгоритмі адаптивного управління визначається результатами оцінки ризиків та співвідношенням інтегрального показника ризику з пороговим значенням. Перехід від стану моніторингу до оцінки ризиків відбувається при появі нових або змінених подій безпеки, що впливають на захищеність активів. Завершення обчислення локальних та інтегральних ризиків є умовою переходу до прийняття управлінських рішень.

Якщо $R_{int} \le R^{int}_{thresholdint}$ і для всіх активів a_i виконується умова $R(a_i) \le R^{local}_{thresholdint}$, система залишається в режимі спостереження та періодичного уточнення параметрів моделі без ініціації додаткових контрзаходів. Якщо ж інтегральний ризик перевищує поріг $R_{int} > R^{int}_{thresholdint}$ або локальний ризик будь-якого активу $R(a_i) > R^{local}_{thresholdint}$, система переходить до стану активного реагування, що включає вибір, реалізацію та подальше коригування контрзаходів як на рівні всієї системи, так і для окремих активів.

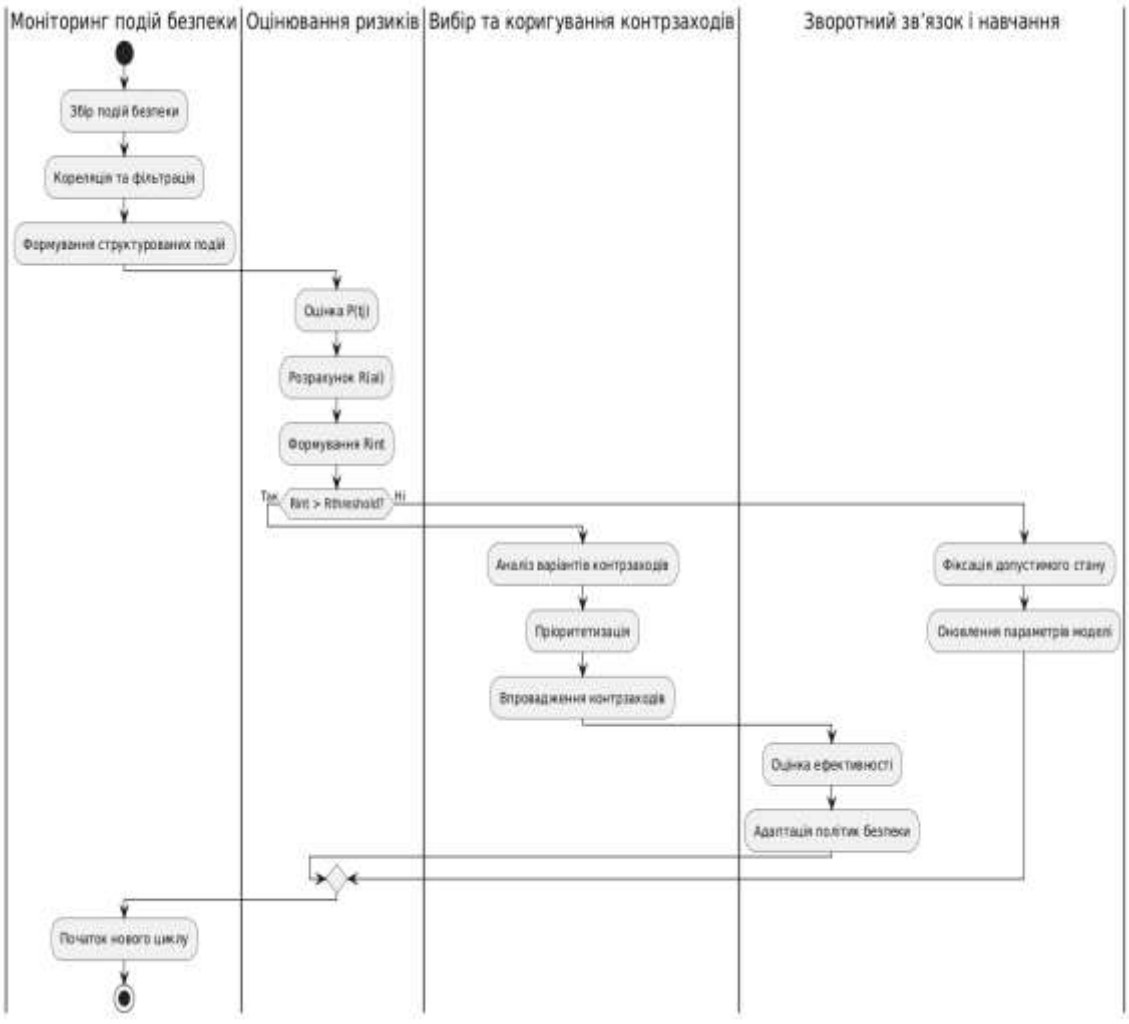

Рисунок 2 — Алгоритм функціонування моделі адаптивного управління кібербезпекою інформаційно-комунікаційних систем

Після застосування контрзаходів система автоматично переходить до етапу аналізу зворотного зв'язку, під час якого визначається, наскільки вдалося знизити ризик. Після цього етапу система повертається до моніторингу, утворюючи замкнений адаптивний цикл, який не має фіксованого завершення.

У разі наближення значень локальних або інтегрального ризиків до порогових меж система може переходити у режим превентивної адаптації, що передбачає підвищення чутливості моніторингу та уточнення параметрів оцінювання без негайного впровадження жорстких контрзаходів. Додатковою умовою зміни стану є суттєва трансформація конфігурації ІКС або критичності активів, що впливає на структуру ризиків і потребує повторної їх переоцінки. Отже, механізм переходів забезпечує гнучке та контекстно-обумовлене реагування системи на зміну внутрішніх і зовнішніх факторів загрозливого середовища.

Реакція алгоритму на зміну рівня ризику

Алгоритм адаптивного управління реагує на зміни рівня ризику залежно від того, як змінюються інтегральний показник ризику та локальні ризики окремих активів порівняно з їхніми допустимими пороговими значеннями. За умов низького рівня інтегрального ризику $R_{int} \le R_{thresholdint}^{int}$ та допустимого ризику всіх активів $R(a_i) \le R_{thresholdint}^{local}$ алгоритм функціонує у режимі стабільного моніторингу, зосереджуючись на накопиченні статистичних даних та уточненні параметрів оцінювання без втручання у конфігурацію інформаційно-комунікаційної системи. У разі зростання інтегрального ризику або перевищення порогового значення локального ризику будь-якого активу алгоритм переходить до режиму превентивної адаптації, що передбачає підвищення чутливості механізмів моніторингу, уточнення ймовірнісних характеристик загроз та аналіз потенційних сценаріїв ескалації ризиків, що дозволяє знизити ймовірність переходу системи у критичний стан. Критичне перевищення порогових значень інтегрального ризику $R_{int} > R_{thresholdint}^{int}$ або локального ризику активу $R(a_i) > R_{thresholdint}^{local}$ розглядається як тригер для активного адаптивного реагування. У цьому режимі алгоритм динамічно обирає та впроваджує контрзаходи, коригує політики безпеки та переглядає пріоритети захисту активів залежно від їхньої пріоритетності. Оцінка ефективності застосованих заходів дозволяє не лише знизити поточний рівень ризику, а й підвищити здатність системи адаптуватися у наступних циклах управління.

Для формалізації логіки роботи моделі адаптивного ризик-орієнтованого управління кібербезпекою інформаційно-комунікаційних систем у вигляді чіткої послідовності дій наведено псевдокод алгоритму:

```
Algorithm: Adaptive risk-oriented cybersecurity management
    Input:
      A – set of assets of the information and communication system
      T – set of threats
      V – set of vulnerabilities
      C – set of available countermeasures
      R_threshold_int – acceptable integral system risk threshold
      R_threshold_local – acceptable local risk threshold
      w_i – criticality weight of asset a_i
    Output:
      Updated security policies
      Optimized set of countermeasures C*
    Initialize security policies and system configuration
    Initialize risk assessment parameters while the information and communication system is operational do
      /* Monitoring and event preprocessing */
```

```
    Collect security events and system state data  Normalize, filter, and correlate security events
  Map events to assets a_i ∈ A and threats t_j ∈ T
    /* Local risk assessment */
    for each asset a_i ∈ A do
      Identify relevant threats T_i ⊆ T
      Estimate probability P(t_j) for each t_j ∈ T_i
      Estimate potential loss L(a_i, t_j)
      Compute local risk:
        R(a_i) = Σ [ P(t_j) · L(a_i, t_j) ], t_j ∈ T_i
    end for
    /* Integral risk calculation */
    Compute integral system risk:
      R_int = Σ [ w_i · R(a_i) ], i = 1…n
    /* Decision-making and adaptation */
    for each asset a_i ∈ A do
      if R(a_i) > R_threshold_local then
            Select countermeasures from C targeting a_i  Prioritize countermeasures according
      to risk reduction effect  Apply selected countermeasures to asset a_i
        Update system configuration and security policies
      end if
    end for
    if R_int > R_threshold_int then
        Select candidate countermeasures from C for system-wide risk reduction  Prioritize
    countermeasures according to risk reduction effect  Apply selected countermeasures C* at
    system level
      Update system configuration and security policies
    end if
    /* Feedback and learning */
  Evaluate effectiveness of applied countermeasures
  Update risk assessment parameters and knowledge base
end while
```

Отже, запропонований алгоритм забезпечує замкнений цикл адаптивного ризик-орієнтованого управління кібербезпекою, у якому результати моніторингу та оцінювання локальних і інтегрального ризиків безпосередньо визначають вибір контрзаходів, оновлення конфігурації та коригування політик безпеки. Важливою особливістю алгоритму є наявність механізму зворотного зв'язку, що дозволяє уточнювати параметри ймовірностей загроз і оцінки збитків, підвищуючи точність розрахунку ризиків у наступних циклах і зменшуючи накопичення неврахованих ризиків у часовому вимірі. Отже, алгоритмічне представлення моделі формує практичну основу для реалізації автоматизованих систем підтримки прийняття рішень у кібербезпеці, а також створює передумови для подальшого кількісного оцінювання ефективності моделі та її порівняння зі статичними підходами в умовах різних сценаріїв загроз і конфігурацій ІКС.

8. Результати

Ефективність розробленої моделі адаптивного управління кібербезпекою оцінювалася за здатністю підтримувати інтегральний ризик R_{int} та локальні ризики активів $R(a_i)$ на рівні нижче встановлених порогових значень ($R^{int}_{thresholdint}$, $R^{local}_{thresholdint}$) у динамічному загрозливому середовищі. Основним критерієм оцінки було порівняння значень інтегрального та локальних ризиків до і після застосування механізмів адаптивного управління, що дозволяє як кількісно, так і якісно визначити ефективність ухвалених рішень.

Порівняння з традиційними статичними методами показало переваги адаптивного підходу: постійне оновлення ймовірностей реалізації загроз $P(t_j)$ та оцінки потенційних збитків $L(a_i, t_j)$ для кожного активу дозволяє приймати обґрунтовані рішення щодо вибору та пріоритезації контрзаходів як на рівні всієї системи, так і окремих активів, що забезпечує зниження інтегрального та локальних ризиків до допустимого рівня. Аналіз різних сценаріїв кібератак підтвердив своєчасне виявлення підвищення ризику та активацію адаптивних механізмів, що гарантує стабільний рівень безпеки ІКС та ефективне використання ресурсів захисту.

Додатково результати підтвердили, що запропонована модель забезпечує стійке утримання інтегрального ризику R_{int} та локальних ризиків активів $R(a_i)$ у межах допустимих порогів $R^{int}_{thresholdint}$ і $R^{local}_{thresholdint}$ за рахунок динамічного оновлення параметрів $P(t_j)$ та $L(a_i, t_j)$ і адаптивного підбору контрзаходів на рівні окремих активів і всієї ІКС. Встановлено, що введення зворотного зв'язку та режиму превентивної адаптації знижує ймовірність переходу системи в критичний стан, оскільки підвищує чутливість моніторингу та забезпечує раннє коригування політик без негайного застосування жорстких контрзаходів. Отже, адаптивна модель зменшує накопичення неврахованих ризиків у часовому вимірі та забезпечує більш раціональне використання ресурсів захисту завдяки пріоритезації контрзаходів за ефектом зниження ризику.

8.1. Обмеження дослідження

Незважаючи на отримані позитивні результати, дослідження має низку обмежень. Запропонована модель представлена на концептуально-алгоритмічному рівні та потребує подальшої експериментальної валідації в реальних інформаційно-комунікаційних середовищах із різними конфігураціями активів і профілями загроз. Точність оцінювання ризиків суттєво залежить від повноти та достовірності вхідних даних, зокрема журналів подій безпеки, аналітичних даних про загрози та експертного визначення вагових коефіцієнтів збитків. Крім того, практичне впровадження моделі потребує розвиненої інфраструктури моніторингу та кореляції подій (SIEM, IDS/IPS, аналітичні модулі), що може обмежувати її застосування в середовищах із низьким рівнем автоматизації процесів кіберзахисту.

8.2. Перспективи подальшого розвитку моделі

Подальші дослідження слід зосередити на вдосконаленні алгоритмічної складової адаптивного управління, зокрема на автоматизації налаштування вагових коефіцієнтів ризику та інтеграції методів машинного навчання для прогнозування кіберінцидентів. Перспективним є також розширення моделі для застосування у хмарних та розподілених системах, де швидкі зміни загроз мають критичне значення. Крім того, важливим напрямом є розробка формалізованих метрик оцінки ефективності контрзаходів і механізмів підтримки прийняття рішень, що підвищить наукову обґрунтованість та практичну цінність даного підходу.

Окрему увагу доцільно приділити розробленню механізмів прогнозування динаміки ризиків на основі аналізу часових рядів і поведінкових характеристик активів, що дозволить переходити від реактивного до проактивного управління кібербезпекою. Перспективним є також використання методів інтелектуальної кореляції подій та пояснюваного штучного інтелекту для підвищення прозорості прийняття управлінських рішень і зменшення залежності від суб'єктивних експертних оцінок. Подальший розвиток моделі може передбачати її масштабування для об'єктів критичної інфраструктури з урахуванням галузевих нормативних вимог і специфіки загроз. Крім того, доцільним є проведення експериментальної апробації моделі в реальних інформаційно-комунікаційних системах підприємств з метою кількісного підтвердження її ефективності в різних сценаріях функціонування.

9. Висновки

Розроблено адаптивну модель ризик-орієнтованого управління кібербезпекою інформаційно-комунікаційних систем, яка об'єднує моніторинг подій безпеки, оцінку ризиків, вибір контрзаходів та механізми зворотного зв'язку в єдиний циклічний процес управління. Запропоновано формалізацію ризику, яка враховує ймовірність реалізації загроз та потенційні збитки для активів, що дозволяє обчислювати інтегральний показник ризику як основний критерій для прийняття управлінських рішень. Побудовані IDEF0-модель та алгоритм функціонування забезпечують структуроване відображення взаємозв'язків між технічними, організаційними та аналітичними складовими кіберзахисту. Результати дослідження підтвердили, що застосування адаптивного підходу дозволяє підтримувати рівень ризику в межах допустимих значень, підвищуючи ефективність реагування на динамічні кіберзагрози.

Практична цінність розробленої моделі полягає у можливості її використання як концептуальної та алгоритмічної основи для побудови систем адаптивного управління кібербезпекою в інформаційно-комунікаційних середовищах різного типу. Модель орієнтована на інтеграцію з існуючими засобами моніторингу та аналізу подій безпеки (SIEM, IDS/IPS), що забезпечує можливість її впровадження без кардинальної зміни архітектури ІКС. Отримані результати можуть бути застосовані при розробленні політик інформаційної безпеки, систем підтримки прийняття рішень та автоматизованих платформ управління кіберризиками.

СПИСОК ДЖЕРЕЛ

1. Melaku H.M. Context-based and adaptive cybersecurity risk management framework. *Risks*. 2023. Vol. 11 (6). Article 101. DOI: https://doi.org/10.3390/risks11060101.
2. Islam S., Basheer N., Papastergiou S., Ciampi M., Silvestri S. Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. *Journal of Reliable Intelligent Environments*. 2025. Vol. 11. Article 12. DOI: https://doi.org/10.1007/s40860-025-00253-3.
3. Cheimonidis P. A dynamic risk assessment and mitigation model for cybersecurity. *Applied Sciences*. 2025. Vol. 15 (4). Article 2171. DOI: https://doi.org/10.3390/app15042171.
4. Minkevics V.A capability-driven automated cybersecurity monitoring and response system. *Frontiers in Computer Science*. 2025. Vol. 7. Article 1692263. DOI: https://doi.org/10.3389/fcomp.2025.1692263.
5. Salamah F.B., Palomino M.A., Craven M.J., Papadaki M., Furnell S. An adaptive cybersecurity training framework for the education of social media users at work. *Applied Sciences*. 2023. Vol. 13 (17). Article 9595. DOI: https://doi.org/10.3390/app13179595.
6. Tkach V., Shemendiuk O., Cherednychenko O. Research on issues of information security risks assessment and management in the security and defense sector and formation of security level indicators. *Cybersecurity: Education, Science, Technique*. 2024. Vol. 2 (26). P. 81–94. DOI: https://doi.org/10.28925/2663-4023.2024.26.636.
7. Symonov A., Klevtsov O., Trubchaninov S., Symonova A. Cybersecurity of NPP Instrumentation and Control Systems: Risks Assessment. *Nuclear and Radiation Safety*. 2022. Vol. 4 (96). P. 62–70. DOI: https://doi.org/10.32918/nrs.2022.4(96).08.
8. Kostiuk Y., Skladannyi P., Rzaieva S., Samoylenko Y., Korshun N. intelligent control and security systems in cyber-physical and cloud environments of smart grid. *Cybersecurity: Education, Science, Technique*. 2025. Vol. 2 (30). P. 125–156. DOI: https://doi.org/10.28925/2663-4023.2025.30.956.
9. Mashkina I., Rzaieva S., Kostiuk Y., Mazur N., Brzhevska Z. Cybersecurity in intelligent transport systems: Current challenges and solutions. *Cybersecurity Providing in Information and Telecommunication Systems 2025. CEUR Workshop Proc*. 2025. P. 1–13. URL: https://ceur-ws.org/Vol-3991/.
10. Rzaieva S.L., Skladannyi P.M., Kostiuk Y.V., Abramov V.O., Kravchenko V.H. Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*. 2025. Vol. 31 (1). P. 23–36. DOI: https://doi.org/10.18372/2225-5036.31.20634.

11. Skladannyi P.M., Kostiuk Y.V., Rzaieva S.L., Samoylenko Y.O., Savchenko T.V. Development of modular neural networks for detecting different classes of network attacks. *Cybersecurity: Education, Science, Technique*. 2025. Vol. 3 (27). P. 534–548. DOI: https://doi.org/10.28925/2663-4023.2025.27.772.
12. Kostiuk Y.V., Bebeshko B.T., Skladannyi P.M., Rzaieva S.L., Khorolska K.V. Optimization of buffer and priorities for ensuring security in bluetooth networks. *Information Systems and Technologies Security*. 2024. Vol. 2 (8). P. 5–16. DOI: https://doi.org/10.17721/ISTS.2024.8.

Стаття надійшла до редакції 12.02.2026 / прийнята до друку 28.04.2026