УДК 004.056:004.052:004.78 DOI: 10.31673/2409-7292.2026.038701

Гречанінов Віктор Федорович
аспірант
Інститут проблем математичних машин і систем НАН України, Київ, Україна
ORCID: 0009-0002-8400-6401
E-mail: vgrechaninov@gmail.com

МЕТОД АДАПТИВНОГО РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ СИТУАЦІЙНИХ ЦЕНТРІВ

У статті розроблено метод адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів в умовах зростання кількості кіберзагроз, ускладнення архітектури інформаційних систем та підвищення вимог до безперервності функціонування критично важливих сервісів. Актуальність дослідження зумовлена необхідністю своєчасного виявлення кіберінцидентів, оцінювання їх впливу на стан інформаційної системи та автоматизованого формування рішень щодо підтримання необхідного рівня гарантоздатності. Метою роботи є розробка методу адаптивного реагування на кіберінциденти на основі інтелектуального аналізу подій безпеки, оцінювання ризиків і динамічного вибору заходів протидії. Проведено аналіз сучасних підходів до забезпечення гарантоздатності інформаційних систем ситуаційних центрів, методів реагування на кіберінциденти та технологій підтримки прийняття рішень. Запропоновано математичну модель оцінювання впливу кіберінцидентів на показники гарантоздатності та формалізовано процес адаптивного реагування. Розроблений метод охоплює моніторинг подій безпеки, класифікацію інцидентів, оцінювання їх критичності, прогнозування розвитку загроз і вибір оптимальної стратегії реагування. Також запропоновано архітектуру інтелектуальної системи підтримки прийняття рішень для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Результати моделювання підтвердили ефективність підходу щодо підвищення рівня гарантоздатності, скорочення часу реагування на кіберінциденти, зменшення ризику порушення функціонування інформаційних ресурсів та підвищення стійкості системи до деструктивних впливів. Отримані результати можуть бути використані під час проєктування, модернізації та експлуатації інформаційних систем ситуаційних центрів, а також для створення інтелектуальних засобів управління кібербезпекою та забезпечення безперервності функціонування.

Ключові слова: ситуаційний центр, гарантоздатність, кіберінцидент, адаптивне реагування, інформаційна система, інтелектуальна система, підтримка прийняття рішень, математична модель, управління ризиками, кібербезпека.

Вступ

Стрімка цифровізація процесів управління, збільшення обсягів даних та зростання кількості кіберзагроз обумовлюють необхідність підвищення ефективності функціонування інформаційних систем ситуаційних центрів. Такі системи використовуються для моніторингу стану об'єктів, аналізу подій, підтримки прийняття управлінських рішень та координації реагування на кризові ситуації [1, 14, 21]. Однією з ключових вимог до їх функціонування є забезпечення гарантоздатності, яка визначає здатність інформаційної системи підтримувати необхідний рівень доступності, надійності, безпеки та безперервності надання сервісів навіть за умов реалізації кіберзагроз, відмов обладнання або програмних збоїв.

Сучасні кіберінциденти характеризуються високою динамічністю, складністю виявлення та здатністю швидко поширюватися між взаємопов'язаними компонентами інформаційної інфраструктури [8, 10, 23]. Традиційні підходи до реагування переважно базуються на статичних правилах та заздалегідь визначених сценаріях протидії, що ускладнює їх застосування в умовах постійної зміни характеристик атак та середовища функціонування системи [1-2, 18, 20]. У зв'язку з цим актуальним науково-практичним завданням є розроблення адаптивних методів реагування на кіберінциденти, здатних автоматично враховувати поточний стан інформаційної системи, рівень ризику, критичність активів та прогнозований розвиток загроз. Особливого значення набуває використання інтелектуальних методів аналізу даних, математичного моделювання та технологій підтримки прийняття рішень [9, 12, 22, 24]. Поєднання засобів моніторингу подій безпеки, моделей оцінювання ризиків та алгоритмів адаптивного вибору стратегій реагування дозволяє формувати більш

ефективні механізми забезпечення гарантоздатності інформаційних систем ситуаційних центрів.

Метою дослідження є розроблення методу адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів на основі інтелектуального аналізу подій безпеки, оцінювання ризиків та автоматизованого формування рішень щодо протидії кіберзагрозам.

Наукова новизна роботи полягає у розробленні методу адаптивного реагування на кіберінциденти, який на відміну від існуючих підходів враховує взаємозв'язок між характеристиками кіберінцидентів, рівнем ризику, станом інформаційної системи та показниками гарантоздатності, що забезпечує динамічний вибір стратегій реагування залежно від поточного контексту функціонування ситуаційного центру.

Теоретичне значення дослідження полягає у розвитку методів інтелектуального аналізу кіберінцидентів, формалізації процесів адаптивного реагування та побудові математичної моделі оцінювання впливу кіберінцидентів на гарантоздатність інформаційних систем ситуаційних центрів. Практичне значення отриманих результатів полягає у можливості використання запропонованого методу під час проєктування, модернізації та експлуатації інформаційних систем ситуаційних центрів, а також під час створення інтелектуальних систем підтримки прийняття рішень у сфері кібербезпеки, моніторингу подій та управління безперервністю функціонування критично важливих інформаційних сервісів.

Постановка проблеми

Сучасні інформаційні системи ситуаційних центрів є складними програмно-технічними комплексами для збору, оброблення, аналізу та візуалізації даних у режимі реального часу [21, 24]. Ефективність їх функціонування залежить від здатності забезпечувати безперервність роботи сервісів, своєчасно виявляти кіберзагрози та оперативно реагувати на кіберінциденти [8, 23]. Водночас ускладнення інформаційних інфраструктур, збільшення кількості взаємопов'язаних компонентів і використання хмарних технологій розширюють поверхню атаки та підвищують ризик порушення функціонування систем.

Однією з ключових характеристик таких систем є гарантоздатність, яка визначає здатність забезпечувати необхідний рівень доступності, надійності, безпеки, цілісності та безперервності функціонування [27]. Реалізація кіберінцидентів може спричиняти втрату доступу до ресурсів, порушення оброблення даних і зниження достовірності аналітичної інформації, що є критичним для ситуаційних центрів.

Існуючі підходи до реагування на кіберінциденти переважно базуються на статичних правилах і сценаріях, що не дозволяє повною мірою враховувати динаміку кіберзагроз, поточний стан системи та зміни показників гарантоздатності [18]. Це знижує ефективність реагування та збільшує ризик порушення безперервності функціонування.

Таким чином, актуальною є задача розроблення методу адаптивного реагування на кіберінциденти, який забезпечуватиме інтелектуальний аналіз подій безпеки, оцінювання їх впливу на гарантоздатність та автоматизований вибір ефективних стратегій реагування [1-2, 7, 23]. Її розв'язання сприятиме підвищенню стійкості інформаційних систем до кіберзагроз і підтриманню необхідного рівня гарантоздатності.

Аналіз останніх досліджень і публікацій

Проблематика забезпечення гарантоздатності інформаційних систем в умовах кіберінцидентів останніми роками привертає значну увагу наукової спільноти. Особливий інтерес становлять дослідження, пов’язані з використанням інтелектуального аналізу даних, машинного навчання та підтримки прийняття рішень.

У роботах Ren, Jin, Niu та Liu [1], а також Klein та Romano [2] запропоновано підходи до автоматизованого вибору стратегій реагування на основі навчання з підкріпленням. Автори продемонстрували ефективність інтелектуальних алгоритмів для підтримки прийняття рішень, однак не врахували показники гарантоздатності інформаційних систем. Дослідження Jha [3] присвячене застосуванню адаптивних алгоритмів штучного інтелекту для відновлення

© Гречанінов В.Ф. Метод адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Сучасний захист інформації, 3(67), 217–232. https://doi.org/10.31673/2409-7292.2026.038701

хмарних сервісів після інцидентів. Незважаючи на ефективність запропонованого підходу, питання комплексного оцінювання гарантоздатності залишилися поза увагою автора.

У роботах Lin та співавторів [4], Tellache та співавторів [5], а також Liu та Anwar [7] використано великі мовні моделі та багатоагентні системи для автоматизації аналізу загроз і реагування на кіберінциденти. Проте ці підходи не враховують вплив інцидентів на гарантоздатність інформаційних систем. Maynard та співавтори [6] запропонували формалізовані моделі кібервторгнень і реагування для критичної інфраструктури, однак задача адаптивного вибору стратегій реагування залежно від поточного стану системи не розглядається. Важливим нормативним документом є NIST SP 800-61 Rev. 3 [8], який визначає сучасні принципи реагування на кіберінциденти, але не містить математичних моделей інтелектуального адаптивного реагування.

Проведений аналіз показав, що існуючі дослідження зосереджені на автоматизації реагування за допомогою машинного навчання, великих мовних моделей і багатоагентних систем [1-7]. Водночас недостатньо дослідженими залишаються питання оцінювання впливу кіберінцидентів на гарантоздатність інформаційних систем ситуаційних центрів та розроблення методів адаптивного реагування, які враховують поточний стан системи, рівень ризику та показники гарантоздатності. Саме усунення цих недоліків становить наукову задачу даного дослідження.

Мета статті

Метою статті є розробка методу адаптивного реагування на кіберінциденти в інформаційних системах ситуаційних центрів, який забезпечує підтримання заданого рівня гарантоздатності шляхом інтелектуального оцінювання стану системи, аналізу характеристик кіберінцидентів та динамічного формування керуючих рішень щодо вибору ефективних заходів протидії кіберзагрозам. Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

– провести аналіз сучасних підходів до забезпечення гарантоздатності інформаційних систем ситуаційних центрів та реагування на кіберінциденти;

– визначити фактори, що впливають на гарантоздатність інформаційних систем в умовах кіберзагроз;

– розробити математичну модель оцінювання впливу кіберінцидентів на стан системи та рівень гарантоздатності;

– формалізувати процес адаптивного реагування з урахуванням характеристик інцидентів, рівня ризику та поточного стану системи;

– розробити метод адаптивного реагування на основі інтелектуального аналізу подій безпеки та динамічного вибору стратегій реагування;

– розробити архітектуру інтелектуальної системи підтримки прийняття рішень щодо реагування на кіберінциденти;

– провести моделювання та оцінити ефективність запропонованого методу за показниками гарантоздатності, оперативності реагування та стійкості до кіберзагроз.

Виклад основного матеріалу дослідження

Для розроблення методу адаптивного реагування на кіберінциденти необхідно формалізувати інформаційну систему ситуаційного центру як об'єкт моніторингу, аналізу та керування. Формалізація дозволяє описати структуру системи, визначити її основні компоненти, параметри функціонування та взаємозв'язки між ними, а також створити математичну основу для оцінювання гарантоздатності, аналізу впливу кіберінцидентів і формування керуючих рішень. У межах дослідження інформаційна система ситуаційного центру розглядається як динамічна багатокомпонентна система, стан якої змінюється під впливом внутрішніх процесів функціонування та зовнішніх кіберзагроз.

Формалізація інформаційної системи ситуаційного центру

Інформаційна система ситуаційного центру являє собою складну програмно-інформаційну систему, призначену для збору, оброблення, аналізу та візуалізації інформації,

© Гречанінов В.Ф. Метод адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Сучасний захист інформації, 3(67), 217–232. https://doi.org/10.31673/2409-7292.2026.038701

необхідної для підтримки прийняття рішень в умовах динамічного середовища [21-22, 24]. Така система розглядається як сукупність взаємопов'язаних компонентів, інформаційних ресурсів, сервісів, користувачів та процесів оброблення даних.

Для формалізації інформаційної системи ситуаційного центру введемо множину:

$$IS = \{N, S, A, U, C\}, \quad (1)$$

де $N = \{n_1, n_2, \dots, n_m\}$ − множина вузлів інформаційної системи, $S = \{s_1, s_2, \dots, s_k\}$ − множина сервісів та програмних модулів, $A = \{a_1, a_2, \dots, a_r\}$ − множина інформаційних активів, $U = \{u_1, u_2, \dots, u_p\}$ − множина користувачів та суб'єктів взаємодії, $C = \{c_1, c_2, \dots, c_l\}$ − множина комунікаційних зв'язків між компонентами системи. Формула визначає структуру інформаційної системи як об'єкта моніторингу, аналізу та адаптивного керування.

У кожний момент часу інформаційна система перебуває у певному функціональному стані, який характеризується множиною параметрів доступності, продуктивності, безпеки та навантаження. Стан системи визначимо вектором:

$$X(t) = \{x_1(t), x_2(t), \dots, x_n(t)\}, \quad (2)$$

де $X(t)$ − вектор стану інформаційної системи у момент часу **t**, $x_i(t)$ − значення і-го параметра функціонування системи, n − кількість контрольованих параметрів. До складу вектора стану можуть входити показники використання процесорних ресурсів, мережевого навантаження, доступності сервісів, кількості активних користувачів, рівня довіри до вузлів та інші характеристики.

Функціонування інформаційної системи відбувається під впливом множини подій безпеки:

$$E = \{e_1, e_2, \dots, e_r\}, \quad (3)$$

де e_r − окрема подія безпеки, зафіксована засобами моніторингу, r − кількість подій, зареєстрованих за певний проміжок часу.

На основі аналізу подій формується інтегральний показник поточного стану інформаційної системи:

$$F(t) = \sum_{i=1}^{n} w_i\, x_i(t) + \sum_{j=1}^{r} v_j\, e_j(t), \quad (4)$$

де $F(t)$ − інтегральна оцінка функціонального стану системи, w_i − ваговий коефіцієнт і-го параметра стану, $x_i(t)$ − значення і-го параметра системи, v_j − ваговий коефіцієнт j-ї події безпеки, $e_j(t)$ − вплив j-ї події безпеки у момент часу t, n − кількість параметрів стану, r − кількість зареєстрованих подій. Вираз інтегрує показники технічного стану системи та параметри кіберобстановки в єдину інтегральну оцінку.

Таким чином, у межах даного підрозділу формалізовано структуру інформаційної системи ситуаційного центру, визначено множину її компонентів, описано вектор поточного стану та введено інтегральний показник функціонування системи, який є основою для подальшого математичного моделювання гарантоздатності та розроблення методу адаптивного реагування на кіберінциденти.

Математична модель оцінювання гарантоздатності

Гарантоздатність інформаційної системи ситуаційного центру доцільно розглядати як інтегральну властивість, що відображає здатність системи забезпечувати безперервне, надійне, безпечне та коректне функціонування в умовах кіберінцидентів [14, 25, 27]. Оцінювання гарантоздатності ґрунтується на математичному моделюванні стану системи, обробленні вхідних даних моніторингу та формуванні кількісної оцінки для подальшого прийняття рішень.

Рівень гарантоздатності інформаційної системи у момент часу **t** подамо у вигляді інтегральної функції:

$$G(t) = \sqrt{\sum_{j=1}^{5} w_j g_j^2(t)}\ , \quad (5)$$

де $G(t)$ – інтегральний рівень гарантоздатності інформаційної системи у момент часу t, $g_j(t)$ – значення j-го показника гарантоздатності у момент часу t, $g_1(t)$ – показник доступності інформаційних сервісів, $g_2(t)$ – показник надійності функціонування компонентів системи, $g_3(t)$ – показник кібербезпеки інформаційної системи, $g_4(t)$ – показник цілісності інформаційних ресурсів, $g_5(t)$ – показник продуктивності системи, w_j – ваговий коефіцієнт j-го показника гарантоздатності, j – номер показника гарантоздатності, $j = 1, \dots, 5$. Залежність реалізує середньоквадратичне агрегування показників гарантоздатності та дозволяє отримати інтегральну оцінку стану інформаційної системи ситуаційного центру. Використання квадратичної форми забезпечує підвищену чутливість моделі до суттєвого погіршення окремих характеристик системи, що є важливим для своєчасного виявлення критичних станів та формування адаптивних керуючих рішень:

$$\sum_{j=1}^{5} w_j = 1,\ w_j \geq 0, \tag{6}$$

де w_j – ваговий коефіцієнт j-го показника гарантоздатності. Умова гарантує коректність формування інтегральної оцінки та узгодженість вагових коефіцієнтів у процесі багатокритеріального оцінювання.

Показник доступності інформаційних сервісів визначимо як відношення кількості працездатних сервісів до загальної кількості сервісів системи:

$$A(t) = \frac{S_a(t)}{S_t(t)}, \tag{7}$$

де $S_a(t)$ – кількість доступних і працездатних сервісів у момент часу t, $S_t(t)$ – загальна кількість сервісів інформаційної системи, $A(t)$ – нормований показник доступності, значення якого належить інтервалу [0; 1].

Показник кібербезпеки системи визначимо з урахуванням кількості виявлених інцидентів, їх критичності та рівня залишкового ризику:

$$B(t) = \frac{1-\left(\sum_{i=1}^{m} K_i(t)\cdot Q_i(t)\right)}{K_{max}}, \tag{8}$$

де $B(t)$ – показник кібербезпеки інформаційної системи, $K_i(t)$ – критичність і-го кіберінциденту у момент часу t, $Q_i(t)$ – імовірність негативного впливу і-го кіберінциденту на систему, m – кількість виявлених кіберінцидентів, K_{max} – максимально допустиме значення сукупного ризикового впливу. Із виразу випливає, що збільшення критичності інцидентів та ймовірності їх реалізації призводить до зменшення значення показника кібербезпеки.

Для оцінювання загального відхилення поточного рівня гарантоздатності від допустимого порогового значення введемо функцію дефіциту гарантоздатності:

$$\Delta G(t) = G_{min} - G(t),\ \text{якщо}\ G(t) < G_{min};\ \ \Delta G(t) = 0,\ \text{якщо}\ G(t) \geq G_{min}, \tag{9}$$

де $\Delta G(t)$ – дефіцит гарантоздатності у момент часу t, G_{min} – мінімально допустимий рівень гарантоздатності інформаційної системи, $G(t)$ – поточний інтегральний рівень гарантоздатності. Формула (9) дозволяє визначити момент, коли система переходить у стан, що потребує адаптивного реагування. Якщо $G(t)$ є меншим за G_{min}, система формує керуючий вплив для відновлення необхідного рівня гарантоздатності. Якщо $G(t)$ не нижчий за порогове значення, активне реагування може бути замінене режимом моніторингу.

Отже, запропонована математична модель дозволяє кількісно оцінювати гарантоздатність інформаційної системи ситуаційного центру з урахуванням доступності, надійності, кібербезпеки, цілісності та продуктивності [21, 27].

Така модель створює основу для подальшого оцінювання впливу кіберінцидентів і вибору адаптивних стратегій реагування в інтелектуальній системі підтримки прийняття рішень.

© Гречанінов В.Ф. Метод адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Сучасний захист інформації, 3(67), 217–232. https://doi.org/10.31673/2409-7292.2026.038701

Модель оцінювання впливу кіберінцидентів

Для забезпечення адаптивного реагування необхідно не лише зафіксувати факт виникнення кіберінциденту, а й кількісно оцінити його вплив на стан інформаційної системи ситуаційного центру [1-2, 8, 23]. Така оцінка має враховувати ймовірність реалізації інциденту, критичність уражених компонентів, масштаб поширення, швидкість розвитку загрози та можливі втрати гарантоздатності [21, 25]. Саме такий підхід базується на формалізації даних, математичному моделюванні та алгоритмічному виборі керуючих рішень.

Для кожного кіберінциденту введемо вектор параметрів:

$$Y_i(t) = \{P_i(t), C_i(t), D_i(t), V_i(t), Z_i(t)\}, \quad (10)$$

де $Y_i(t)$ – вектор параметрів і-го кіберінциденту у момент часу t, $P_i(t)$ – імовірність реалізації або повторного прояву інциденту, $C_i(t)$ – критичність ураженого компонента або активу, $D_i(t)$ – рівень деструктивного впливу інциденту, $V_i(t)$ – швидкість поширення наслідків інциденту в системі, $Z_i(t)$ – ступінь охоплення системи інцидентом. Формула дозволяє подати кіберінцидент як багатовимірний об'єкт аналізу, що надалі використовується для класифікації, прогнозування та вибору стратегії реагування.

Інтегральний рівень небезпечності і-го кіберінциденту визначимо як зважену згортку його параметрів:

$$H_i(t) = \lambda_1 P_i(t) + \lambda_2 C_i(t) + \lambda_3 D_i(t) + \lambda_4 V_i(t) + \lambda_5 Z_i(t), \quad (11)$$

де $H_i(t)$ – інтегральний рівень небезпечності і-го кіберінциденту, $\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5$ – вагові коефіцієнти параметрів кіберінциденту, $P_i(t), C_i(t), D_i(t), V_i(t), Z_i(t)$ – нормовані параметри інциденту. Вагові коефіцієнти у формулі (10) визначають значущість кожного параметра для конкретної інформаційної системи ситуаційного центру та мають задовольняти умову: $\sum_{j=1}^{5} \lambda_j = 1, \ \lambda_j \geq 0$. Вплив кіберінциденту на гарантоздатність інформаційної системи визначимо через втрату рівня гарантоздатності:

$$L_i(t) = H_i(t) \cdot M_i(t) \cdot (1 - R_p(t)), \quad (12)$$

де $L_i(t)$ – величина втрати гарантоздатності внаслідок і-го кіберінциденту, $H_i(t)$ – інтегральний рівень небезпечності інциденту, $M_i(t)$ – коефіцієнт важливості ураженого компонента для функціонування ситуаційного центру, $R_p(t)$ – рівень готовності системи до протидії інциденту, $(1 - R_p(t))$ – залишкова вразливість системи після врахування наявних засобів захисту. Залежність відображає вплив рівня підготовленості системи на величину втрат гарантоздатності.

Сукупний вплив усіх активних кіберінцидентів на гарантоздатність інформаційної системи визначимо як:

$$L\Sigma(t) = \sum_{i=1}^{m} L_i(t) \cdot \rho_i(t), \quad (13)$$

де $L\Sigma(t)$ – сукупна втрата гарантоздатності інформаційної системи у момент часу t, $L_i(t)$ – втрата гарантоздатності внаслідок і-го кіберінциденту, $\rho_i(t)$ – коефіцієнт взаємного впливу і-го інциденту з іншими інцидентами або компонентами системи, m – кількість активних кіберінцидентів.

Коефіцієнт $\rho_i(t)$ дозволяє врахувати каскадний ефект, коли один кіберінцидент може посилювати дію інших інцидентів або впливати на декілька взаємопов'язаних компонентів інформаційної системи. Це особливо важливо для ситуаційних центрів, де відмова одного сервісу або каналу оброблення даних може спричинити порушення роботи суміжних підсистем.

Отже, запропонована модель забезпечує кількісне оцінювання небезпечності кіберінцидентів, втрат гарантоздатності та їх сукупного впливу на інформаційну систему ситуаційного центру [14, 23]. Це створює основу для формування методу адаптивного

© Гречанінов В.Ф. Метод адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Сучасний захист інформації, 3(67), 217–232. https://doi.org/10.31673/2409-7292.2026.038701

реагування, у якому керуючі рішення приймаються з урахуванням поточного стану системи, характеристик інцидентів і прогнозованої зміни гарантоздатності.

Метод адаптивного реагування на кіберінциденти

На основі розроблених моделей гарантоздатності та оцінювання впливу кіберінцидентів пропонується метод адаптивного реагування, який забезпечує автоматизований вибір керуючих рішень залежно від поточного стану інформаційної системи ситуаційного центру, характеристик кіберінцидентів та прогнозованої зміни рівня гарантоздатності [20, 23]. На відміну від традиційних підходів, запропонований метод використовує інтелектуальний механізм оцінювання ситуації та динамічного коригування стратегій реагування, що відповідає концепції підтримки прийняття рішень [10, 16].

Введемо множину можливих стратегій реагування:

$$D = \{d_1, d_2, \dots, d_k\}, \tag{14}$$

де D – множина допустимих стратегій реагування, d_1 – моніторинг ситуації, d_2 – локалізація інциденту, d_3 – ізоляція уражених компонентів, d_4 – переналаштування ресурсів, d_5 – відновлення функціонування сервісів, d_k – інші керуючі дії. Кожна стратегія характеризується власною ефективністю, вартістю реалізації та впливом на гарантоздатність системи.

Для оцінювання доцільності застосування певної стратегії сформуємо функцію корисності керуючого рішення:

$$U(d_i, t) = \omega_1 \Delta G(d_i, t) - \omega_2 C(d_i, t) + \omega_3 E(d_i, t) - \omega_4 T(d_i, t), \tag{15}$$

де $U(d_i, t)$ – інтегральна функція корисності стратегії реагування d_i у момент часу t, $\Delta G(d_i, t)$ – прогнозоване підвищення рівня гарантоздатності інформаційної системи після реалізації стратегії d_i, $C(d_i, t)$ – витрати обчислювальних, мережевих та організаційних ресурсів, необхідних для реалізації стратегії d_i, $E(d_i, t)$ – ефективність усунення наслідків кіберінциденту та відновлення працездатності системи, $T(d_i, t)$ – час реалізації стратегії реагування, $\omega_1, \omega_2, \omega_3, \omega_4$ – вагові коефіцієнти критеріїв оцінювання, $\omega_1 + \omega_2 + \omega_3 + \omega_4 = 1,\ \omega_1 \geq 0,\ j = 1, \dots, 4$. Залежність реалізує багатокритеріальне оцінювання альтернативних стратегій реагування. При цьому критерії підвищення гарантоздатності та ефективності усунення наслідків інциденту збільшують значення функції корисності, тоді як витрати ресурсів і тривалість реалізації стратегії зменшують її. Це дозволяє здійснювати адаптивний вибір керуючого рішення на основі компромісу між ефективністю реагування, швидкістю виконання та витратами ресурсів інформаційної системи ситуаційного центру.

Оптимальна стратегія реагування визначається як рішення, що максимізує функцію корисності:

$$d^* = \arg\max_{d_i \in D} U(d_i, t), \tag{16}$$

де d^* – оптимальна стратегія реагування, яка забезпечує максимальне значення функції корисності серед множини допустимих стратегій D, $U(d_i, t)$ – функція корисності стратегії d_i.

Після вибору стратегії здійснюється адаптивне оновлення стану інформаційної системи. Новий рівень гарантоздатності визначається за формулою:

$$G(t+1) = G(t) + \mu \Delta G(t) - v L\Sigma(t), \tag{17}$$

де $G(t+1)$ – прогнозований рівень гарантоздатності після виконання керуючого рішення, $G(t)$ – поточний рівень гарантоздатності, $\Delta G(t)$ – приріст гарантоздатності внаслідок реалізації обраної стратегії, $L\Sigma(t)$ – сукупні втрати гарантоздатності від активних кіберінцидентів, μ – коефіцієнт ефективності реагування, v – коефіцієнт впливу інцидентів на систему.

Для реалізації адаптивного механізму керування вагові коефіцієнти критеріїв коригуються залежно від накопиченого досвіду функціонування системи:

$$\omega_j(t+1) = \omega_j(t) + \eta\,[e(t) - \hat{e}(t)]\,x_j(t), \tag{18}$$

де $\omega_j(t+1)$ – оновлене значення вагового коефіцієнта, $\omega_j(t)$ – поточне значення вагового коефіцієнта, η – коефіцієнт адаптації (навчання) системи, $e(t)$ – фактичний результат реагування, $\hat{e}(t)$ – прогнозований результат реагування, $x_j(t)$ – значення j-го критерію оцінювання. Співвідношення реалізує механізм адаптації параметрів системи підтримки прийняття рішень. За наявності відхилення між прогнозованими та фактичними результатами реагування система автоматично коригує вагові коефіцієнти, підвищуючи ефективність подальших рішень.

На рис. 1 наведено структурну схему методу адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Метод реалізує послідовний цикл моніторингу подій безпеки, виявлення та аналізу кіберінцидентів, оцінювання їх впливу на гарантоздатність системи, формування та оцінювання стратегій реагування, вибору оптимального керуючого рішення і його реалізації [7, 16, 24]. Особливістю методу є наявність механізму адаптації параметрів та бази знань, що забезпечують накопичення досвіду реагування і підвищення ефективності прийняття рішень в умовах динамічної зміни кіберобстановки.

Рис. 1. Структурна схема методу адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів

Запропонований метод належить до класу адаптивних інтелектуальних систем підтримки прийняття рішень та поєднує математичне моделювання, багатокритеріальне оцінювання, адаптивне керування й елементи машинного навчання [10, 20]. Формування керуючих впливів здійснюється на основі аналізу даних моніторингу, оцінювання стану системи та прогнозування зміни рівня гарантоздатності, що забезпечує адаптацію до змін кіберобстановки та підвищення ефективності реагування на кіберінциденти.

Отже, запропонований метод адаптивного реагування поєднує математичні моделі оцінювання гарантоздатності, аналізу впливу кіберінцидентів та механізми інтелектуального вибору стратегій реагування [14, 21, 24]. Це дозволяє забезпечити динамічне формування керуючих рішень з урахуванням поточного стану системи, рівня ризику та прогнозованої зміни гарантоздатності, що створює основу для побудови інтелектуальних систем підтримки прийняття рішень у ситуаційних центрах.

Архітектура інтелектуальної системи підтримки прийняття рішень

Для реалізації запропонованого методу адаптивного реагування на кіберінциденти розроблено архітектуру інтелектуальної системи підтримки прийняття рішень, призначену для забезпечення гарантоздатності інформаційних систем ситуаційних центрів [7-8, 24, 26]. Архітектура побудована за модульним принципом і забезпечує безперервний цикл моніторингу, аналізу, оцінювання та формування керуючих рішень.

© Гречанінов В.Ф. Метод адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Сучасний захист інформації, 3(67), 217–232. https://doi.org/10.31673/2409-7292.2026.038701

Функціонування системи починається з модуля моніторингу подій безпеки, який здійснює збір і попередню обробку даних із журналів подій, мережевих сенсорів та інших джерел телеметрії [15, 17, 19]. Отримана інформація надходить до модуля аналізу кіберінцидентів, де виконується класифікація подій та формування вектора параметрів інциденту.

Далі модуль оцінювання ризику визначає рівень небезпечності інцидентів, прогнозує можливі наслідки їх розвитку та оцінює втрати гарантоздатності [22, 27]. Одночасно модуль оцінювання гарантоздатності розраховує інтегральний показник гарантоздатності та визначає поточний стан системи.

Результати аналізу передаються до модуля підтримки прийняття рішень, який формує множину можливих стратегій реагування та виконує їх оцінювання за функцією корисності [24, 26]. Після вибору оптимальної стратегії вона передається до модуля адаптивного реагування для локалізації інциденту, мінімізації його наслідків і відновлення нормального функціонування системи.

Важливою складовою архітектури є база знань, що містить правила реагування, історію інцидентів та результати попередніх рішень [16, 24]. Це забезпечує адаптацію системи до нових загроз і підвищення ефективності прийняття рішень.

На рис. 2 наведено трирівневу архітектуру інтелектуальної системи підтримки прийняття рішень. Перший рівень забезпечує збір, попередню обробку та аналіз даних кібербезпеки, що надходять із засобів моніторингу [17, 19]. Другий рівень реалізує оцінювання ризику, гарантоздатності інформаційної системи та формування оптимальної стратегії реагування на основі механізмів підтримки прийняття рішень. Третій рівень відповідає за адаптивне реагування на кіберінциденти, накопичення знань і навчання системи шляхом коригування параметрів на основі результатів попереднього функціонування [16]. Архітектура забезпечує безперервний цикл моніторингу, аналізу, прийняття рішень, реагування та адаптації до змін кіберобстановки.

Рис. 2. Архітектура інтелектуальної системи підтримки прийняття рішень для адаптивного реагування на кіберінциденти

Запропонована архітектура поєднує математичне моделювання, інтелектуальний аналіз даних, підтримку прийняття рішень та адаптивне керування, що дозволяє використовувати її як основу для побудови інтелектуальних інформаційних систем ситуаційних центрів.

Алгоритм роботи методу адаптивного реагування

Запропонований метод адаптивного реагування функціонує у циклічному режимі та забезпечує безперервний моніторинг стану інформаційної системи ситуаційного центру

© Гречанінов В.Ф. Метод адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Сучасний захист інформації, 3(67), 217–232. https://doi.org/10.31673/2409-7292.2026.038701

[8, 21]. На початковому етапі здійснюється збір і аналіз подій безпеки, після чого виконується виявлення та класифікація кіберінцидентів [17, 19]. Далі оцінюється рівень їх небезпечності та визначається вплив на гарантоздатність інформаційної системи.

На основі отриманих результатів розраховується поточний рівень гарантоздатності та формується множина можливих стратегій реагування [21, 24]. Для кожної стратегії виконується оцінювання ефективності, після чого обирається найбільш доцільне керуюче рішення. Реалізація обраної стратегії спрямована на локалізацію інциденту, мінімізацію його наслідків та відновлення нормального функціонування системи.

Після завершення реагування результати виконаних дій використовуються для оновлення бази знань і коригування параметрів системи, що забезпечує адаптацію до змін кіберобстановки та підвищення ефективності подальшого реагування [24]. Алгоритм роботи запропонованого методу наведено в алгоритмі 1.

Algorithm 1. Adaptive Incident Response Method
Input:
Current system state X(t);
set of security events E;
knowledge base KB.
Output:
Optimal response strategy d*.
1. Collect current monitoring data from the information system.
2. Analyze security events received from monitoring tools.
3. Detect and classify cyber incidents.
4. Form the incident parameter vector Yi(t).
5. Calculate the incident hazard level Hi(t).
6. Estimate the impact of the incident on system dependability.
7. Calculate the current dependability level G(t).
8. Generate the set of possible response strategies D.
9. For each response strategy, calculate its utility value U(di, t).
10. Select the optimal response strategy d*.
11. Implement the selected response strategy.
12. Localize the incident and minimize its consequences.
13. Restore the normal functioning of the information system.
14. Update the knowledge base KB.
15. Adjust system parameters for the next monitoring cycle.
16. Return to continuous monitoring.

Результати експериментального дослідження

Для перевірки ефективності запропонованого методу адаптивного реагування було проведено моделювання функціонування інформаційної системи ситуаційного центру в умовах реалізації різних типів кіберінцидентів [1-2, 23]. Моделювання виконувалося в середовищі Python 3.12 із використанням бібліотек NumPy та Pandas.

Таблиця 1

Сценарії моделювання інформаційної системи ситуаційного центру

Сценарій	Характеристика сценарію	Тип кіберінциденту	Рівень небезпечності	Очікуваний вплив на гарантоздатність
S1	Штатний режим функціонування системи	Відсутній	Низький	Відсутній
S2	Перевантаження мережевої інфраструктури та сервісів запитами	DDoS-атака	Високий	Зниження доступності сервісів
S3	Отримання несанкціонованого доступу до критичного вузла системи	Компрометація вузла	Високий	Порушення цілісності та конфіденційності даних
S4	Одночасна реалізація декількох взаємопов'язаних загроз	Комплексний кіберінцидент	Критичний	Комплексне зниження доступності, цілісності та продуктивності системи

Для оцінювання ефективності запропонованого методу було сформовано набір сценаріїв, що відображають різні умови функціонування інформаційної системи ситуаційного центру [21-22]. Характеристики сценаріїв наведено в табл. 1.

Сценарій S1 використовується як базовий та відображає нормальне функціонування інформаційної системи без реалізації кіберзагроз. Сценарій S2 моделює DDoS-атаку, спрямовану на перевантаження мережевих ресурсів та зниження доступності інформаційних сервісів. У сценарії S3 розглядається компрометація критичного вузла інформаційної інфраструктури, що може призвести до порушення цілісності та конфіденційності даних. Найбільш складним є сценарій S4, який моделює комплексний кіберінцидент із одночасною реалізацією декількох типів загроз, що впливають на різні компоненти інформаційної системи та призводять до суттєвого зниження рівня гарантоздатності [6, 14, 23]. Використання наведених сценаріїв дозволяє комплексно оцінити ефективність запропонованого методу адаптивного реагування в умовах різного рівня складності кіберінцидентів та визначити його вплив на показники гарантоздатності інформаційної системи.

Для оцінювання ефективності запропонованого методу виконано порівняння з традиційним статичним підходом та підходом, заснованим на використанні набору правил реагування (Rule-Based Response) [8, 18]. Основними критеріями оцінювання обрано рівень гарантоздатності після реагування та середній час реагування на кіберінцидент. Результати порівняльного аналізу наведено в табл. 2.

Таблиця 2

Порівняння методів реагування

Метод	Гарантоздатність	Час реагування, с	Точність вибору стратегії	Рівень зниження ризику
Статичний	0,72	15,4	0,71	28 %
Rule-Based Response	0,81	11,8	0,84	47 %
Запропонований метод	0,92	6,3	0,95	68 %

Результати, наведені в табл. 2, свідчать про переваги запропонованого методу над існуючими підходами. Використання адаптивного механізму прийняття рішень дозволило підвищити інтегральний рівень гарантоздатності інформаційної системи до значення 0,92, що на 27,8 % більше порівняно зі статичним підходом та на 13,6 % більше порівняно з Rule-Based Response. Одночасно середній час реагування скоротився до 6,3 с, що забезпечує більш оперативну локалізацію кіберінцидентів та зменшення їх негативного впливу на функціонування системи.

Як видно з рис. 3, запропонований метод забезпечує найвище значення гарантоздатності (0,92) та найменший час реагування (6,3 с) серед досліджуваних підходів, що підтверджує ефективність використання інтелектуального механізму підтримки прийняття рішень і адаптивного вибору стратегій реагування.

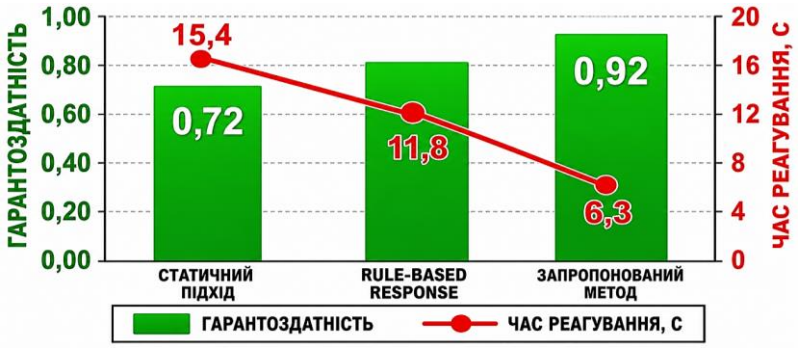

Рис. 3. Порівняння показників гарантоздатності та часу реагування для різних методів реагування

Додатково було проведено оцінювання рівня гарантоздатності для кожного зі сценаріїв моделювання. Отримані результати наведено в табл. 3.

Таблиця 3

Рівень гарантоздатності за різних сценаріїв

Сценарій	Статичний підхід	Rule-Based Response	Запропонований метод
S1	0,95	0,96	0,98
S2	0,71	0,82	0,92
S3	0,69	0,79	0,90
S4	0,54	0,67	0,87

Аналіз результатів показує, що найбільший ефект від застосування запропонованого методу спостерігається в умовах складних кіберінцидентів. Зокрема, для сценарію S4 рівень гарантоздатності зріс із 0,54 до 0,87, що свідчить про високу ефективність адаптивного вибору стратегій реагування та використання інтелектуального механізму підтримки прийняття рішень.

Результати, наведені на рис. 4, підтверджують ефективність запропонованого методу в умовах різного рівня складності кіберінцидентів. Навіть у сценарії S4, який характеризується комплексним впливом взаємопов'язаних загроз, рівень гарантоздатності залишається істотно вищим порівняно з альтернативними підходами [6, 14, 23]. Це свідчить про доцільність використання інтелектуальних механізмів підтримки прийняття рішень та адаптивного керування процесом реагування в інформаційних системах ситуаційних центрів.

Рис. 4. Рівень гарантоздатності інформаційної системи за сценаріями S1–S4

У середньому запропонований метод забезпечив підвищення рівня гарантоздатності на 21,6 % порівняно з Rule-Based Response та на 35,7 % порівняно зі статичним підходом. Одночасно середній час реагування було скорочено більш ніж у 2 рази, що підтверджує ефективність використання інтелектуального механізму підтримки прийняття рішень та адаптивного вибору стратегій реагування. Для більш детального аналізу процесу реагування було досліджено зміну рівня гарантоздатності інформаційної системи на різних етапах розвитку кіберінциденту. Результати моделювання наведено в табл. 4.

Таблиця 4

Динаміка зміни рівня гарантоздатності інформаційної системи
на етапах реагування на кіберінцидент

Етап реагування	Статичний підхід	Rule-Based Response	Запропонований метод
Нормальний стан	0,95	0,95	0,95
Виявлення інциденту	0,78	0,84	0,91
Розвиток інциденту	0,62	0,76	0,89
Локалізація	0,58	0,74	0,90
Відновлення	0,72	0,81	0,92

Дані табл. 4 свідчать, що найбільше зниження гарантоздатності спостерігається на етапах розвитку та локалізації кіберінциденту [14, 21]. Запропонований метод забезпечує

найменші втрати гарантоздатності на всіх етапах реагування та демонструє найкращі показники відновлення функціонального стану системи. Зокрема, на етапі локалізації рівень гарантоздатності становить 0,90, тоді як для Rule-Based Response цей показник дорівнює 0,74, а для статичного підходу – лише 0,58. Отримані результати підтверджують ефективність адаптивного вибору стратегій реагування та використання інтелектуальних механізмів підтримки прийняття рішень.

Результати, наведені на рис. 5, демонструють динаміку зміни рівня гарантоздатності інформаційної системи під час розвитку кіберінциденту. Запропонований метод забезпечує найменше зниження гарантоздатності на етапах розвитку та локалізації інциденту, а також найшвидше відновлення працездатності системи після реалізації заходів реагування [23]. На відміну від статичного підходу та Rule-Based Response, запропонований метод підтримує рівень гарантоздатності вище 0,89 протягом більшості етапів реагування, що підтверджує ефективність використання інтелектуальних механізмів підтримки прийняття рішень та адаптивного керування процесом реагування.

Рис. 5. Зміна рівня гарантоздатності інформаційної системи під час розвитку кіберінциденту

Отримані результати підтверджують доцільність використання математичних моделей оцінювання гарантоздатності, аналізу впливу кіберінцидентів та адаптивного керування процесом реагування [21, 27]. Запропонований метод забезпечує підвищення стійкості інформаційних систем ситуаційних центрів до кіберзагроз, скорочення часу реагування та підтримання необхідного рівня гарантоздатності в умовах динамічної зміни кіберобстановки.

Обговорення

Отримані результати підтверджують ефективність запропонованого методу адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів [1-2, 14]. На відміну від традиційних статичних підходів і методів, заснованих на фіксованих правилах реагування, запропонований підхід враховує поточний стан інформаційної системи, характеристики кіберінцидентів та прогнозовану зміну рівня гарантоздатності [8, 21, 23]. Подібний підхід до динамічного оцінювання стану системи та формування адаптивних рішень розглядається також у роботах, присвячених інтелектуальному керуванню захистом складних інформаційних середовищ і безперервному оцінюванню подій безпеки [11, 13]. Проведене моделювання показало, що використання математичних моделей оцінювання гарантоздатності та впливу кіберінцидентів дозволяє формувати більш обґрунтовані керуючі рішення та скорочувати час реагування на загрози [27]. Найбільший ефект спостерігається в умовах складних і комплексних кіберінцидентів, коли запропонований метод забезпечує суттєво вищий рівень гарантоздатності порівняно зі статичним підходом і Rule-Based Response.

© Гречанінов В.Ф. Метод адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Сучасний захист інформації, 3(67), 217–232. https://doi.org/10.31673/2409-7292.2026.038701

Особливістю запропонованого підходу є поєднання багатокритеріального оцінювання стану системи, адаптивного вибору стратегій реагування та механізму коригування параметрів на основі накопиченого досвіду функціонування. Це дозволяє розглядати розроблений метод як складову інтелектуальних систем підтримки прийняття рішень у сфері кібербезпеки [10-11, 24]. Крім того, використання механізмів адаптації на основі аналізу подій безпеки узгоджується з сучасними концепціями безперервного контролю безпеки та динамічного управління доступом у рамках Zero Trust-підходу [13]. Отримані результати підтверджують доцільність використання методів математичного моделювання, аналізу даних та адаптивного керування для забезпечення гарантоздатності інформаційних систем ситуаційних центрів в умовах динамічної зміни кіберсередовища.

Висновки та перспективи подальших досліджень

У статті розв'язано актуальну науково-практичну задачу розроблення методу адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. У результаті дослідження проведено аналіз сучасних підходів до реагування на кіберінциденти та забезпечення гарантоздатності інформаційних систем. Формалізовано інформаційну систему ситуаційного центру, розроблено математичну модель оцінювання гарантоздатності та модель оцінювання впливу кіберінцидентів на стан системи. На основі запропонованих моделей розроблено метод адаптивного реагування, який забезпечує автоматизований вибір стратегій реагування залежно від поточного стану системи, характеристик кіберінцидентів та прогнозованої зміни рівня гарантоздатності.

Також запропоновано архітектуру інтелектуальної системи підтримки прийняття рішень і алгоритм функціонування методу. Результати експериментального дослідження підтвердили ефективність запропонованого підходу щодо підвищення рівня гарантоздатності, скорочення часу реагування на кіберінциденти та зменшення ризику порушення функціонування інформаційних ресурсів ситуаційного центру.

Перспективи подальших досліджень полягають у розробленні методів прогнозування розвитку кіберінцидентів на основі машинного навчання, інтеграції технологій штучного інтелекту для автоматичного формування стратегій реагування, а також створенні програмного прототипу інтелектуальної системи підтримки прийняття рішень для практичного впровадження в інформаційних системах ситуаційних центрів.

Перелік посилань

1. Ren, S., Jin, J., Niu, G., & Liu, Y. (2025). ARCS: Adaptive reinforcement learning framework for automated cybersecurity incident response strategy optimization. Applied Sciences, 15(2), Article 951. https://doi.org/10.3390/app15020951.

2. Klein, T., & Romano, G. (2025). Optimizing cybersecurity incident response via adaptive reinforcement learning. Journal of Advances in Engineering and Technology, 2(1). https://doi.org/10.62177/jaet.v2i1.212.

3. Jha, N. N. (2025). Accelerating cloud outage recovery through adaptive AI: A reinforcement learning approach. European Journal of Computer Science and Information Technology, 13(26), 1–10. https://doi.org/10.37745/ejcsit.2013/vol13n26110.

4. Lin, X., Zhang, J., Deng, G., Liu, T., Zhang, T., Guo, Q., & Chen, R. (2025). IRCopilot: Automated incident response with large language models. arXiv. https://arxiv.org/abs/2505.20945.

5. Tellache, A., Korba, A. A., Mokhtari, A., Moldovan, H., & Ghamri-Doudane, Y. (2025). Advancing autonomous incident response: Leveraging LLMs and cyber threat intelligence (arXiv:2508.10677). arXiv. https://arxiv.org/abs/2508.10677.

6. Maynard, P., Cherdantseva, Y., Shaked, A., Burnap, P., & Mehmood, A. (2025). Consistent and compatible modelling of cyber intrusions and incident response demonstrated in the context of malware attacks on critical infrastructure (arXiv:2505.16398). arXiv. https://arxiv.org/abs/2505.16398.

7. Liu, Z., & Anwar, A. (2025). AutoBnB-RAG: Enhancing multi-agent incident response with retrieval-augmented generation (arXiv:2508.13118). arXiv. https://arxiv.org/abs/2508.13118.

8. Nelson, A., et al. (2025). Incident response recommendations and considerations for cybersecurity risk management (NIST SP 800-61 Rev. 3). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/61/r3/final.

9. Складанний, П. М., Костюк, Ю. В., Рзаєва, С. Л., Самойленко, Ю. В., & Савченко, Т. В. (2025). Розробка модульних нейронних мереж для виявлення різних класів мережевих атак. Кібербезпека: освіта, наука, техніка, 3(27), 534-548. https://doi.org/10.28925/2663-4023.2025.27.772.

© Гречанінов В.Ф. Метод адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Сучасний захист інформації, 3(67), 217–232. https://doi.org/10.31673/2409-7292.2026.038701

10. Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems, 67, 6969–7055. https://doi.org/10.1007/s10115-025-02429-y.

11. Костюк, Ю. В., Складанний, П. М., Рзаєва, С. Л., Самойленко, Ю. В., & Коршун, Н. В. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. Кібербезпека: освіта, наука, техніка, 2(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956.

12. Khatri, V., Agarwal, G., Gupta, A., & Sanghi, A. (2024). Machine learning and artificial intelligence in cybersecurity: Innovations and challenges. In Proceedings of the International Conference on Advances in Computing, Communication and Technology (pp. 732–737). IEEE. https://doi.org/10.1109/ICACCTech65084.2024.00122.

13. Складанний, П. М., Костюк, Ю. В., & Рзаєва, С. Л. (2026). Безперервна оцінка доступу в Zero Trust Access Management на основі подієвих сигналів безпеки та динамічного керування сесіями. Математичні машини і системи, 1, 29-46. https://doi.org/10.34121/1028-9763-2026-1-29-46.

14. Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. ACM Computing Surveys, 56(8), 1–48. https://doi.org/10.1145/3649218.

15. Костюк, Ю. В., Рзаєва, С. Л., & Рзаєв, Д. О. (2026). Інтелектуальний аналіз мережевого трафіку для виявлення інцидентів інформаційної безпеки. Наука і техніка сьогодні, 2(56), 1909-1928. https://doi.org/10.52058/2786-6025-2026-2(56)-1909-1928.

16. Calvo Ibañez, A., Preetam, S., & Compastié, M. (2025). Explainable AI for cybersecurity decisions: Challenges and opportunities. In Artificial Intelligence for Cybersecurity (pp. 385–408). Elsevier. https://doi.org/10.1016/B978-0-44-329135-7.00018-7.

17. Костюк, Ю. В., & Складанний, П. М. (2026). Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103-118. https://doi.org/10.31673/2409-7292.2026.011393.

18. Joseph, J., Aleke, N., & Onyeanisi, O. P. (2025). Intelligent incident response systems using machine learning. Mikailalsys Journal of Advanced Engineering International, 2(1). https://doi.org/10.58578/MJAEI.v2i1.4540.

19. Костюк, Ю. В., Складанний, П. М., & Рзаєва, С. Л. (2026). Управління якістю сповіщень у SIEM на основі ризик-орієнтованого оцінювання та зворотного зв'язку SOC. Український науковий журнал інформаційної безпеки, 31(3), 151–163. https://doi.org/10.18372/2225-5036.31.21161.

20. Hammad, A. A., Ahmed, S. R., Abdul-Hussein, M. K., Ahmed, M. R., Majeed, D. A., & Algburi, S. (2024). Deep reinforcement learning for adaptive cyber defense in network security. In Proceedings of the Cognitive Models and Artificial Intelligence Conference (pp. 292–297).

21. Рзаєва, С. Л., Литвин, О. С., Складанний, П. М., Костюк, Ю. В., & Рзаєв, Д. О. (2026). Модель адаптивного управління кібербезпекою інформаційно-комунікаційних систем на основі ризик-орієнтованого підходу. Математичні машини і системи, 2, 92–109. https://doi.org/10.34121/1028-9763-2026-2-92-109.

22. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., & Korshun, N. (2024). Models and algorithms for analyzing information risks during the security audit of personal data information system. In Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024) (Vol. 3925, pp. 155–171). CEUR Workshop Proceedings.

23. Farzaan, M. A. M., Ghanem, M. C., El-Hajjar, A., & Ratnayake, D. N. (2025). AI-powered system for an efficient and effective cyber incidents detection and response in cloud environments. IEEE Transactions on Machine Learning in Communications and Networking, 3, 623–643. https://doi.org/10.1109/TMLCN.2025.3564912.

24. Kostiuk, Y., Skladannyi, P., Sokolov, V., & Vorokhob, M. (2025). Models and technologies of cognitive agents for decision-making with integration of artificial intelligence. In Proceedings of the Modern Data Science Technologies Doctoral Consortium (MoDaST 2025) (Vol. 4005, pp. 82-96). CEUR Workshop Proceedings.

25. Shevchenko, S., Zhdanova, Y., Kryvytska, O., & Shevchenko, H. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In Cybersecurity Providing in Information and Telecommunication Systems II (Vol. 3826, pp. 356–362).

26. Kostiuk, Y. (2025). Multi-agent system for detecting and counteracting attacks on the enterprise information system. In Insider Threats and Security in Corporations (pp. 205–232). https://doi.org/10.36690/ITSC-205-232.

27. Dacorogna, M., Debbabi, N., & Kratz, M. (2023). Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. European Journal of Operational Research, 311(2), 707–721. https://doi.org/10.1016/j.ejor.2023.05.003.

Victor Hrechaninov
postgraduate
Institute of Mathematical Machines and Systems Problems, Kyiv, Ukraine
ORCID: 0009-0002-8400-6401
E-mail: vgrechaninov@gmail.com

ADAPTIVE CYBER INCIDENT RESPONSE METHOD FOR ENSURING DEPENDABILITY OF INFORMATION SYSTEMS IN SITUATION CENTERS

The paper develops an adaptive cyber incident response method aimed at ensuring the dependability of information systems used in situation centers under conditions of increasing cyber threats, growing complexity of information system architectures, and higher requirements for the continuity of critical services. The relevance of the study is determined by the need for timely detection of cyber incidents, assessment of their impact on the state of information systems, and automated generation of decisions to maintain the required level of dependability. The purpose of the research is to develop an adaptive cyber incident response method based on intelligent security event analysis, risk assessment, and dynamic selection of countermeasures. A review of current approaches to ensuring the dependability of information systems in situation centers, cyber incident response methods, and decision support technologies is conducted. A mathematical model for assessing the impact of cyber incidents on dependability indicators is proposed, and the adaptive response process is formalized. The developed method includes security event monitoring, incident classification, criticality assessment, threat evolution forecasting, and selection of an optimal response strategy. In addition, an architecture of an intelligent decision support system for ensuring the dependability of information systems in situation centers is proposed. Simulation results confirmed the effectiveness of the approach in increasing the level of dependability, reducing cyber incident response time, decreasing the risk of disruption of information resources, and improving system resilience to destructive impacts. The obtained results can be applied in the design, modernization, and operation of information systems in situation centers, as well as in the development of intelligent cybersecurity management tools and mechanisms for ensuring operational continuity.

Keywords: situation center, dependability, cyber incident, adaptive response, information system, intelligent system, decision support, mathematical model, risk management, cybersecurity.

Надійшла до редакції (Received): 25.08.2026
Прийнята до друку (Accepted): 08.09.2026
Опубліковано онлайн (Available online): 15.09.2026

УДК 004.056.53:004.89 DOI: 10.31673/2409-7292.2026.037206

Лозова Ірина Леонідівна
кандидат технічних наук, доцент кафедри Управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-7224-4763
E-mail: illozovaya@gmail.com

Скулиш Євген Деонізійович
доктор юридичних наук, професор, керівник наукового центру національної безпеки і права
Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», Київ, Україна
ORCID: https://orcid.org/0000-0001-9646-8473
E-mail: us5519mail@gmail.com

ПІДХІД ДО АВТОМАТИЗАЦІЇ ПЕРВИННОГО РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В SOC НА ОСНОВІ ІНТЕГРАЦІЇ SIEM ТА МЕХАНІЗМІВ АВТОМАТИЗОВАНОЇ ОБРОБКИ

У статті запропоновано підхід до автоматизації первинного реагування на кіберінциденти в центрі моніторингу безпеки (SOC) на основі інтеграції системи SIEM із програмним модулем автоматизованої обробки та зовнішніми джерелами даних. Запропонований підхід передбачає автоматизоване отримання та структурування інформації про інциденти з IBM QRadar через REST API, її збагачення результатами перевірки IP-адрес, характеристиками активів і даними про вразливості з Nessus Vulnerability Management. На основі сформованого контексту здійснюється визначення пріоритетності інцидентів, формування заявок, надсилання сповіщень аналітику та оновлення відповідної інформації в SIEM. Особливістю запропонованого підходу є автоматизація стандартизованих процедур первинного опрацювання без необхідності впровадження повноцінної SOAR-платформи, із збереженням контролю аналітика SOC над критичними діями реагування.

© Гречанінов В.Ф. Метод адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Сучасний захист інформації, 3(67), 217–232.
https://doi.org/10.31673/2409-7292.2026.038701