Оцінювання допустимості альтернатив реагування на кіберінциденти в органах військового управління

УДК 004.056.5

Геннадій Рибачок[1]

[1]*Національний університет оборони України, ryba4okgen@gmail.com*

Кіберінциденти у секторі безпеки і оборони дедалі частіше мають не лише технічний, а й управлінський зміст [1]. Для органів військового управління Збройних Сил України важливо встановити не тільки факт порушення функціонування інформаційної системи, а й допустимі варіанти реагування з урахуванням часу, ресурсів, повноважень, режимно-безпекових обмежень і залишкового ризику. За таких умов технічно можлива дія не завжди є управлінсько прийнятною, тому в системі підтримки прийняття рішень потрібна окрема процедура оцінювання допустимості альтернатив реагування. Сучасні стандарти й рекомендації з управління кіберінцидентами визначають загальну логіку підготовки, виявлення, аналізу, реагування, відновлення та післяінцидентного удосконалення [2, 3, 4].

Водночас вони не розв'язують повною мірою завдання вибору конкретної альтернативи дій у військово-управлінському контексті. Після оцінювання інциденту суб'єкт управління має отримати не загальну вказівку на потребу реагування, а множину дій, з якої вилучено варіанти, неприйнятні за наявних умов. Метою тез є обґрунтування методичного підходу до оцінювання допустимості альтернатив реагування на кіберінциденти в системі підтримки прийняття рішень органів військового управління Збройних Сил України. Наукова новизна підходу полягає в розмежуванні технічно можливих і управлінсько допустимих альтернатив реагування шляхом попередньої перевірки за повноважними, часовими, ресурсними, режимно-безпековими, ризиковими та управлінськими обмеженнями.

Альтернатива реагування розглядається як можливий варіант дій щодо нейтралізації кіберінциденту, сформований з урахуванням результату оцінювання інциденту, початкового управлінського стану, вимог до ефективності реагування, допустимого залишкового ризику та профілю умов реагування. Базова множина альтернатив не повинна одразу ототожнюватися з рекомендованим рішенням. Вона є початковим простором можливих дій, який потребує перевірки на допустимість і здійсненність. У загальному вигляді перевірку доцільно подати як формування множини допустимих альтернатив:

$$A_i feas = \{a_{ij} \in A_i^0 \mid Feas_i(a_{ij}, \Pi_i, E_i req, Risk_i adm) = 1\},$$

де a_{ij} — j-та альтернатива реагування для і-го кіберінциденту; A_i^0 — базова множина альтернатив; Π_i — профіль умов реагування; вимоги до ефективності реагування визначають очікуваний результат нейтралізації; допустимий залишковий ризик задає межу прийнятності наслідків; предикат Feas визначає допустимість і здійсненність альтернативи. Якщо значення предиката дорівнює 1, альтернатива може бути передана на критеріальне оцінювання.

До основних груп умов допустимості належать повноважна й процедурна допустимість, часова здійсненність, ресурсна забезпеченість, режимно-безпекова сумісність, ризикова прийнятність та управлінська придатність.

Повноважна умова не допускає варіантів, що виходять за межі компетенції суб'єкта рішення або порушують порядок ескалації. Часова умова відсікає дії, які не забезпечують досягнення потрібного рівня нейтралізації в наявних часових межах. Ресурсна умова перевіряє наявність сил, засобів, фахівців і доступу до необхідних даних. Режимно-безпекова умова враховує обмеження щодо інформації, режимів роботи систем і недопущення вторинних ризиків. Ризикова умова пов'язує альтернативу з допустимим залишковим ризиком.

Управлінська придатність показує, чи не погіршує дія керованість, інформаційний обмін або виконання завдань більше, ніж сам інцидент. Для об'єктів критичної інфраструктури та систем, що забезпечують військове управління, такий підхід дає можливість відокремити технічно можливі дії від управлінсько прийнятних [1, 4]. Наприклад, локалізація інциденту може бути технічно швидкою, але неприйнятною, якщо вона зупиняє критичний процес, потребує неузгодженого втручання або створює надмірний залишковий ризик. Саме тому оцінювання допустимості має передувати критеріальному вибору рекомендованої альтернативи. Якщо після перевірки множина допустимих альтернатив є порожньою, система підтримки прийняття рішень не повинна імітувати наявність готового рішення. У такому випадку результатом має бути висновок про відсутність допустимих альтернатив у наявному профілі умов реагування з пропозицією уточнення даних, перегляду ресурсних меж, формування комбінованих варіантів або ескалації рішення. Отже, оцінювання допустимості альтернатив є необхідною проміжною ланкою між формуванням базового простору дій і вибором рекомендованого рішення щодо нейтралізації кіберінциденту.

Його використання підвищує відтворюваність підготовки управлінського рішення, забезпечує пояснюваність відбору альтернатив і зберігає принципову межу: інформаційна технологія формує обґрунтовану рекомендацію, а остаточне рішення залишається за уповноваженим суб'єктом військового управління.

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 15.05.2026).
2. ISO/IEC 27035-1:2023. Information technology — Information security incident management — Part 1: Principles and process. URL: https://www.iso.org/standard/78973.html (дата звернення: 15.05.2026).
3. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management. NIST SP 800-61 Rev. 3. 2025. URL: https://doi.org/10.6028/NIST.SP.800-61r3 (дата звернення: 15.05.2026).
4. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. NIST, 2024. URL: https://doi.org/10.6028/NIST.CSWP.29 (дата звернення: 15.05.2026).