КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1311
УДК 004.056.5:355

Рибачок Геннадій Іванович
ад'юнкт кафедри кіберборотьби
Національний університет оборони України, Київ, Україна
ORCID:0009-0002-8513-5133
ryba4okgen@gmail.com

Микусь Сергій Анатолійович
доктор технічних наук, професор,
заступник начальника Інституту інформаційно-комунікаційних технологій та кібероборони
Національний університет оборони України, Київ, Україна
ORCID:0000-0002-7103-4166
serg.mikus@gmail.com

ЧИННИКИ І КОНТЕКСТ ПРИЙНЯТТЯ РІШЕНЬ ОРГАНАМИ ВІЙСЬКОВОГО УПРАВЛІННЯ ПІД ЧАС КІБЕРІНЦИДЕНТІВ

Анотація. Реагування на кіберінциденти в інтересах органів військового управління (ОВУ) Збройних Сил України відбувається в умовах обмеженого часу, неповноти даних і обов'язкової координації між кількома суб'єктами національної системи реагування. Для ОВУ результатом є не фіксація технічних ознак події, а підготовлене рішення щодо реагування, яке визначає дозволені й заборонені дії, їх часові вікна, пріоритети та обмеження. Чинна нормативно-організаційна рамка (Закон України № 2163-VIII, Стратегія кібербезпеки України, постанови Кабінету Міністрів України № 1471 і № 1533 від листопада 2025 року) та міжнародні процесні моделі (NIST CSF 2.0, NIST SP 800-61 Rev. 3, серія ISO/IEC 27035) докладно регламентують послідовність дій реагування, проте не виокремлюють умови прийняття рішення як самостійний об'єкт опису. Через це різні підрозділи можуть спиратися на відмінні припущення щодо обмежень, пріоритетів і наслідків, що знижує зіставність рішень навіть для технічно подібних інцидентів. У статті запропоновано таксономію внутрішніх і зовнішніх чинників впливу на рішення та структуру контексту прийняття рішення у вигляді узгодженого пакета вхідних даних, що декомпонується на контекст місії, нормативні обмеження, контекст активів і дані про кіберзагрози. Для зменшення невизначеності введено атрибут статусу (відомо, припущено, невідомо) і вимогу артефактного підтвердження ключових параметрів, а для простежуваності – рольову рамку суб'єктів, які формують і погоджують елементи контексту. Побудовано матрицю відповідності «чинник – елемент контексту – наслідок для рішення» та мінімальний перелік артефактів як практичний інструмент підготовки рішення у контурі реагування. Отримані результати відмежовують опис інциденту від умов прийняття рішення, підвищують зіставність рішень для типових класів інцидентів і утворюють термінологічно-концептуальну основу для подальшого обґрунтування системи показників і критеріїв оцінювання реагування. Запропонований апарат не дублює моделі пріоритезації та вибору альтернатив, а передує їм, фіксуючи вхідні умови, на яких такі моделі ґрунтуються.

Ключові слова: кіберінцидент; органи військового управління; прийняття рішень; контекст рішення; чинники впливу; контур реагування; артефакт; кіберрозвідка; критична інфраструктура.

ВСТУП

Постановка проблеми. Повномасштабна збройна агресія Російської Федерації перетворила інформаційно-комунікаційні системи на окремий театр дій, де кібератаки синхронізуються з діями противника, а реагування ведеться в умовах дефіциту часу, неповноти даних і одночасних подій у різних сегментах військових мереж. Для органів військового управління результатом опрацювання кіберінциденту є не фіксація його технічних ознак, а підготовлене рішення щодо реагування: які дії санкціонувати, дозволити, відкласти чи заборонити, у яких часових вікнах, з якими пріоритетами та обмеженнями, на підставі яких відомостей і за участі яких суб'єктів. Закон України «Про основні засади

забезпечення кібербезпеки України» розглядає кіберінцидент не як вузькотехнічну подію, а як явище, що може загрожувати інформаційно-комунікаційним системам, державним інформаційним ресурсам та виконанню функцій держави, і відносить реагування до контуру національної безпеки й оборони [1]. Стратегія кібербезпеки України переводить цю правову основу у площину державної політики, закріплюючи стримування, кіберстійкість і взаємодію як функціональні засади національної системи кібербезпеки [2].

Процедурний рівень визначають дві постанови Кабінету Міністрів України, ухвалені наприкінці 2025 року. Постанова № 1471 від 13 листопада 2025 року встановила порядок взаємодії суб'єктів національної системи реагування із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними та розвідувальними органами [3]. Постанова № 1533 від 26 листопада 2025 року затвердила Національний план реагування на кіберінциденти, кібератаки та кіберзагрози, у структурі якого виокремлено підготовку до реагування, виявлення, аналіз та інформування, стримування, усунення наслідків і відновлення, а також аналіз ефективності заходів [4]. Для оборонного сектору цей акт встановлює, що заходи реагування, які можуть спричинити тимчасові обмеження роботи систем Міністерства оборони, здійснюються за погодженням з ним, а в частині, що стосується Збройних Сил України, – за погодженням з Генеральним штабом [4]. Для об'єктів критичної інфраструктури загальні вимоги до кіберзахисту, зокрема режими доступу й обмеження, визначено окремою постановою [5]. Водночас наведені акти показують, що рішення ОВУ формується не ізольовано, а в середовищі множинних залежностей і зовнішніх вимог до взаємодії.

Міжнародні підходи описують реагування як кероване, а не ситуативне. NIST Cybersecurity Framework 2.0 розміщує функції Respond і Recover в одному контурі з Govern, Identify, Protect і Detect, пов'язуючи якість реагування з визначеністю ролей, порядку обігу інформації та пріоритетів захисту [6]. NIST SP 800-61 Rev. 3 конкретизує цю рамку, інтегруючи реагування в цикл управління кіберризиками і наголошуючи на координації, пріоритезації та документуванні дій [7]. Серія ISO/IEC 27035, чинна в Україні як ДСТУ ISO/IEC 27035-1:2024 та ДСТУ ISO/IEC 27035-2:2024, задає принципи та процес керування інцидентами [8] і вимоги до планування, готовності й розподілу ролей [9]. Ці документи докладно регламентують, як організоване реагування, але умови, за яких приймається конкретне рішення, у них присутні лише опосередковано. Через відсутність уніфікованого опису цих умов виникає розрив: одна й та сама подія за різного контексту місії, стану активів чи нормативних обмежень потребує різних рішень, проте підстави для такого розрізнення не зафіксовані у відтворюваній формі.

Аналіз останніх досліджень і публікацій. Операційний шар реагування найповніше поданий у третій частині серії ISO/IEC 27035, яка охоплює виявлення, повідомлення, первинне сортування подій, аналіз, локалізацію, усунення наслідків і відновлення [10]. Складні та розподілені інциденти виходять за межі однієї організації, тому четверта частина серії присвячена координованому опрацюванню інцидентів кількома організаціями і ролі координаційної команди [11]. Практичний вимір розгортання спроможності доповнює методичний звіт ENISA щодо створення CSIRT і SOC, який показує послідовність нарощування спроможностей і зв'язок між структурою команди, процесами та операційним середовищем [12]. Ці джерела докладно описують процес і організаційну готовність, але розглядають їх з боку виконавця реагування, а не з боку умов, у яких готується управлінське рішення.

Прив'язку рішень до місії та зон відповідальності формалізовано в підході управління ризиками. NIST SP 800-37 орієнтує організаційні рішення із захисту та реагування на місію і функції та закріплює відповідальності, що забезпечують керованість і простежуваність дій [13]. Для відомостей про загрози істотною є їх артефактність: настанови NIST щодо обміну інформацією про кіберзагрози підкреслюють, що саме форматовані й відтворювані артефакти уможливлюють координацію, повторну перевірку та обмін між суб'єктами [14]. Ці роботи показують, що рішення спирається не лише на опис події, а й на структуровані вхідні дані з визначеним джерелом і рівнем довіри, проте не зводять такі дані до єдиного пакета, придатного для підготовки рішення.

Окремий напрям стосується вимірювання та оцінювання реагування. Настанови NIST SP 800-55 описують відбір показників безпеки та побудову програми вимірювань, відділяючи показники перебігу від показників результату [15, 16]. Моделі пріоритезації інцидентів розв'язують суміжну задачу впорядкування подій за важливістю. Національна система оцінювання кіберінцидентів NCISS агрегує кілька груп параметрів у підсумковий рівень ризику й стандартизує первинне ранжування [17]. Підхід Crown Jewels Analysis зміщує фокус з інциденту на критичні для місії активи та залежності, компрометація яких має непропорційний вплив на виконання завдань [18]. Багатофакторна пріоритезація поєднує технічну небезпеку, національні рівні критичності та багатокритеріальне впорядкування в одну процедуру [19]. Ці моделі продуктивні, але кожна з них приймає вхідні умови як задані: оцінка ризику, критичність активу чи ваги критеріїв уже мають бути сформовані до застосування методу. Питання про

те, які чинники й у якому структурованому вигляді утворюють ці вхідні умови для ОВУ, у розглянутих роботах системно не ставиться.

Мета статті. Уніфікація подання чинників і контексту, що впливають на прийняття рішень ОВУ під час кіберінцидентів, та обґрунтування структурованого пакета вхідних даних для підготовки такого рішення у контурі реагування, фазову логіку якого описують процесні моделі керування інцидентами [7, 8]. Для досягнення мети розв'язано такі завдання: систематизувати внутрішні та зовнішні чинники і визначити механізми їхнього впливу на допустимі дії, пріоритети й часові вікна; сформувати структуру контексту прийняття рішення з декомпозицією на контекст місії, нормативні обмеження, контекст активів і дані про кіберзагрози; визначити підхід до фіксації статусу елементів контексту та їх артефактного підтвердження; окреслити рольову рамку суб'єктів і запропонувати мінімальний перелік артефактів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Терміни та припущення. Під кіберінцидентом у статті розуміється подія або сукупність подій у кіберпросторі, що порушує або створює загрозу порушення конфіденційності, цілісності чи доступності інформації та потребує організованого реагування; таке трактування узгоджується із законодавчим визначенням [1] та з логікою процесного керування інцидентами [8]. Рішення щодо реагування (управлінське рішення, УР) трактується як санкціонований ОВУ вибір допустимого набору дій у контурі реагування, який визначає перелік дозволених і заборонених дій, їх часові вікна, пріоритети та обмеження, підставові артефакти й коло залучених суб'єктів.

Контур керованого реагування використовується як узагальнений опис процесу, у якому з пакета вхідних даних формується рішення, далі воно реалізується як заходи реагування і приводить до результатів – локалізації, усунення наслідків, відновлення та звітування. Фазова логіка контуру відповідає Національному плану реагування (підготовка; виявлення, аналіз та інформування; стримування; усунення наслідків і відновлення; аналіз ефективності) [4] та операційному опису реагування у стандарті [10]. Контекст прийняття рішення визначається як узгоджений і відтворюваний пакет вхідних даних, достатній для підготовки рішення. Засадничою є відмінність між описом інциденту, тобто тим, що зафіксовано на рівні ознак події, і умовами прийняття рішення, тобто пріоритетами, обмеженнями та станом активів, за яких допускаються певні дії. Прив'язка умов до місії та відповідальностей спирається на ризик-орієнтований підхід [13].

Статус позначає рівень визначеності елемента контексту за шкалою «відомо/припущено/невідомо» і фіксує, чи підтверджено елемент артефактно. Суб'єкт означає роль, що створює або постачає артефакт, перевіряє чи погоджує його або має повноваження санкціонувати рішення або його частину. Артефакт розуміється як документований відтворюваний об'єкт (запис, витяг, звіт), який можна передати між суб'єктами, повторно перевірити та використати як підставу для санкціонування дій; вимога артефактності випливає з процесних підходів до керування інцидентами [7, 9].

Таксономія чинників впливу на рішення. Таксономія пояснює, чому однаковий за технічними ознаками інцидент потребує різних рішень. Наприклад, одночасні DDoS-атака на вузол зв'язку, фішинг з ескалацією привілеїв і підозра на компрометацію сегмента забезпечення можуть мати близьку технічну природу, проте рішення щодо них відрізнятиметься залежно від того, чи зачеплено критичний для поточного завдання сервіс і які часові вікна задає обстановка. Чинники поділено на внутрішні, керовані або частково керовані ОВУ, і зовнішні, зумовлені середовищем, нормативними вимогами та міжсуб'єктною взаємодією (табл. 1).

Серед внутрішніх чинників визначальними є місійні цілі та пріоритети, які задають допустимий рівень ризику, компроміс між швидкістю і глибиною дій та часові вікна втручання [13]. Організаційна готовність і доступні спроможності реагування визначають, чи реалістично виконати дію у потрібний час [9, 12]. Стан і критичність активів задають допустимість ізоляції чи обмеження доступу та поріг прийнятної деградації функцій [18]. Якість і доступність даних про інцидент впливають на статус елементів контексту та на ризик хибних рішень [7], а внутрішні правила ескалації й санкціонування формують часові вікна через затримки погоджень [9].

Серед зовнішніх чинників ключовими є нормативно-правові вимоги до реагування і взаємодії, які встановлюють обов'язкові повідомлення й погодження та звужують множину допустимих дій [1, 3, 4]. Вимоги до кіберзахисту об'єктів критичної інфраструктури накладають режимні обмеження на дії щодо відповідних активів [5]. Міжсуб'єктна координація може звужувати часові вікна та потребувати узгодження артефактів [3, 11]. Динаміка загрози та невизначеність середовища змінюють оцінку ризику наслідків і потребу у превентивних діях [14, 19], а стан зовнішньої інфраструктури впливає на реалізовність дій і вибір резервних режимів [6].

Механізми впливу зводяться до чотирьох типів: зміна множини допустимих дій через нормативні обмеження та ресурсно-технічний стан [5, 9]; перерозподіл пріоритетів через контекст місії [13]; зсув часових вікон через процедури погодження та координацію [4, 11]; зміна оцінки ризику наслідків через дані про загрози й контекст активів, де статус робить явною невизначеність рішення [14].

Таблиця 1

Таксономія чинників впливу на рішення ОВУ під час кіберінцидентів

Група	Чинник	Стислий опис	Переважний механізм впливу на рішення
Внутрішні	Місійні цілі та пріоритети	поточні завдання, їх критичність і темп виконання	пріоритети, допустимий ризик, часові вікна [13]
Внутрішні	Організаційна готовність і спроможності	плани, чергові зміни, ресурси, канали зв'язку	множина виконуваних дій [9, 12]
Внутрішні	Стан і критичність активів	цінність, залежності, резерви, допустимість ізоляції	допустимість дій, поріг деградації [18]
Внутрішні	Якість і доступність даних про інцидент	повнота телеметрії, доказовість, доступ до матеріалів	статус елементів, ризик хибних рішень [7]
Внутрішні	Правила ескалації та санкціонування	пороги, ланцюг погоджень, відповідальні	часові вікна, закріплення відповідальності [9]
Зовнішні	Нормативно-правові вимоги до реагування і взаємодії	дефініції, порядок взаємодії та реагування	легітимність дій, обов'язкові повідомлення [1, 3, 4]
Зовнішні	Вимоги до кіберзахисту критичної інфраструктури	загальні вимоги, режими доступу	режимні обмеження дій щодо об'єктів [5]
Зовнішні	Міжсуб'єктна координація та залежності	узгодження даних і дій із зовнішніми учасниками	звуження часових вікон, синхронізація [3, 11]
Зовнішні	Динаміка загрози та невизначеність (ТІ)	еволюція загроз, масштаб компрометації	оцінка ризику наслідків, превентивні дії [14, 19]
Зовнішні	Стан зовнішньої інфраструктури та середовища	зв'язок, енергетика, постачальники	реалізовність дій, вибір резервних режимів [6]

Контекст прийняття рішення як пакет вхідних даних. Контекст подається як структурований пакет, достатній для підготовки рішення, з декомпозицією на контекст місії, нормативні обмеження, контекст активів і дані про кіберзагрози. Кожен елемент має змістові атрибути, статус, артефакт-підтвердження та прив'язку до відповідального суб'єкта. Така побудова відображає логіку контуру реагування (рис. 1): пакет контексту живить підготовку рішення, рішення розгортається у заходи реагування за фазами Національного плану, а результати разом з аналізом ефективності повертаються у контекст для наступних рішень [4, 8].

Контекст місії містить очікуваний ефект реагування, поточні пріоритети, часові обмеження, межі прийнятності наслідків і вимоги до координації; його прив'язка до функцій управління спирається на ризик-орієнтований підхід [13]. Нормативні обмеження охоплюють правові вимоги взаємодії та звітування [1, 3, 4], режимні обмеження щодо об'єктів критичної інфраструктури [5] та внутрішні процедури санкціонування [9]. Контекст активів описує перелік уражених активів і сервісів, їх критичність, залежності, поточний стан і доступні резерви, причому критичність доцільно визначати за внеском активу у виконання завдань, а не за абстрактною важливістю [18]. Дані про кіберзагрози подають гіпотезу щодо типу загрози та можливих наслідків, джерела й актуальність відомостей, їх релевантність і ключові припущення, а також індикатори, що підтверджують або спростовують гіпотезу; цінність цього елемента визначається не лише змістом, а й артефактністю та статусом [14].

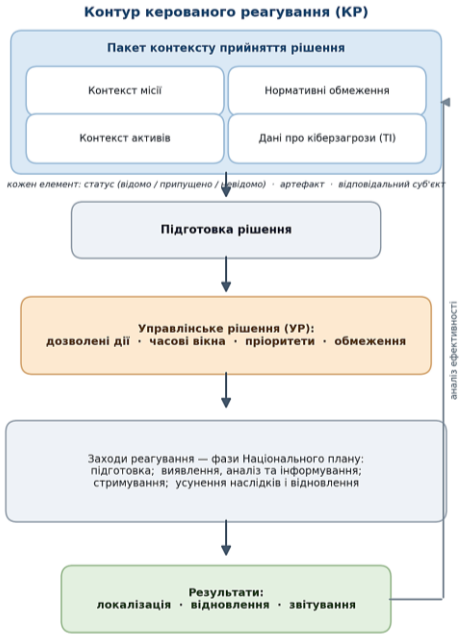

Рис. 1. Контур керованого реагування: від пакета контексту до рішення та результатів

Для застосування у контурі реагування статус фіксують за трьома рівнями. Рівень «відомо» означає, що параметр підтверджено артефактно і допускає повторну перевірку. Рівень «припущено» вказує, що параметр спирається на гіпотезу або непряме підтвердження. Рівень «невідомо» фіксує брак підтвердження або обмеженість доступу. Для ключових атрибутів визначають мінімальний доказ, тобто конкретний артефакт, що підтверджує параметр, відповідно до вимоги документування в керуванні інцидентами [7, 9].

Простежуваність забезпечує рольова рамка, у якій кожен артефакт контексту має власника і погоджувача. Доцільно розрізняти суб'єкта, що реєструє інцидент і постачає первинні дані; аналітика, що формує відомості про загрозу й пропонує варіанти дій; власника активу, що підтверджує критичність і допустимість впливу на доступність; уповноваженого на нормативні обмеження, що підтверджує правові й процедурні рамки; уповноваженого на рішення, що санкціонує дії та визначає пріоритети. Конкретний склад суб'єктів і їх повноваження залежать від внутрішніх регламентів і потребують узгодження з порядком міжсуб'єктної взаємодії [3].

Матриця відповідності та мінімальний перелік артефактів. Матриця відповідності пов'язує чинник, елемент контексту, що його покриває, і тип наслідку для рішення (табл. 2). Вона застосовується як інструмент уніфікації: під час підготовки рішення фіксують, який чинник потрібно врахувати, який елемент контексту його охоплює та якого наслідку для рішення слід очікувати. Перед санкціонуванням рішення перевіряють мінімальну узгодженість вхідних даних: контекст місії та нормативні обмеження підтверджені або явно позначені як припущені чи невідомі; контекст активів уточнено до рівня оцінки допустимості ключових дій; дані про загрозу мають артефактну опору; для критичних параметрів визначено статус і закріплено відповідального суб'єкта.

Таблиця 2

Матриця відповідності «чинник – елемент контексту – наслідок для рішення»

Чинник	Елемент контексту, що його покриває	Тип наслідку для рішення
Місійні цілі та пріоритети	Контекст місії	перерозподіл пріоритетів, межі прийнятності наслідків [13]
Стан і критичність активів	Контекст активів	допустимість ізоляції/обмеження, поріг деградації [18]
Нормативні вимоги до взаємодії	Нормативні обмеження	обов'язкові повідомлення та погодження, межі дій [1, 3, 4]
Вимоги до критичної інфраструктури	Нормативні обмеження/контекст активів	режимні обмеження дій щодо об'єктів [5]

Чинник	Елемент контексту, що його покриває	Тип наслідку для рішення
Динаміка загрози (TI)	Дані про кіберзагрози	зміна оцінки ризику, потреба превентивних дій [14, 19]
Якість даних про інцидент	усі елементи через атрибут статусу	рівень визначеності, потреба дозбору перед критичними діями [7]
Міжсуб'єктна координація	Нормативні обмеження/процес	зсув часових вікон, синхронізація артефактів [3, 11]
Правила ескалації та санкціонування	Нормативні обмеження	часові вікна погоджень, закріплення відповідальності [9]

Мінімальний перелік артефактів контексту впорядковує підготовку рішення у вигляді переліку, придатного для роботи чергових змін і аналітичних груп. До нього доцільно віднести: опис цілей і пріоритетів реагування на поточному етапі з явним статусом; витяг із застосовних нормативних вимог і порядків взаємодії [3, 4]; внутрішній витяг із процедур санкціонування ключових дій [9]; картку ураженого активу або сервісу з критичністю, залежностями та допустимістю обмежень [18]; аналітичну довідку щодо загрози з гіпотезою, припущеннями, джерелами та релевантністю [14]; перелік артефактів-доказів, що підтверджують або спростовують гіпотезу; відомість простежуваності із зазначенням авторів і погоджувачів артефактів; протокол прийнятого рішення з переліком санкціонованих дій, часових вікон, обмежень і статусів критичних припущень [7]. Такий перелік не передбачає обчислення показників чи побудови оптимізаційної постановки; його призначення – забезпечити повноту та узгодженість вхідних даних до того, як буде застосовано моделі оцінювання та пріоритезації [15, 17, 19].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розв'язано завдання уніфікації подання чинників і контексту, що визначають прийняття рішень ОВУ під час реагування на кіберінциденти. Запропоновано таксономію чинників, яка відокремлює внутрішні, керовані ОВУ, від зовнішніх, середовищних, і дозволяє ідентифікувати джерела обмежень для дій у контурі реагування. Обґрунтовано структуру контексту прийняття рішення як цілісного пакета вхідних даних, що відмежовує опис технічної сутності інциденту від управлінських умов його вирішення. Введено атрибут статусу та рольову рамку суб'єктів, що підвищує простежуваність і робить явними припущення, на яких ґрунтується рішення. Сформовано матрицю відповідності та мінімальний перелік артефактів, що утворюють методичне підґрунтя для стандартизації роботи чергових змін і аналітичних груп.

На відміну від процесних моделей реагування [7, 8, 10] і моделей оцінювання та пріоритезації [15], [17, 18, 19], які приймають вхідні умови як задані, запропонований апарат описує самі ці умови у відтворюваній формі і тим самим передує оцінюванню, а не конкурує з ним. Це відрізняє роботу від задач вибору допустимих альтернатив і багатокритеріального впорядкування інцидентів, що розглядаються окремо. Перспективи подальших досліджень полягають у переході від структури контексту до системи показників і критеріїв оцінювання реагування [15, 16] та до формалізованих процедур пріоритезації інцидентів і вибору варіантів реагування з урахуванням ресурсних обмежень [17, 19], що відповідає логіці розгортання інформаційної технології підтримки прийняття рішень в інтересах ОВУ Збройних Сил України.

Фінансування. Дослідження виконано без зовнішнього фінансування.

Конфлікт інтересів. Автори заявляють про відсутність конфлікту інтересів.

Внесок авторів. Рибачок Г. І. – концептуалізація, методологія, формальний аналіз, написання первинного проєкту рукопису. Микусь С. А. – наукове керівництво, концептуалізація, валідація, написання (критичне рецензування та редагування).

Використання інструментів штучного інтелекту. Допоміжні інструменти ШІ використано лише для технічного оформлення рукопису (упорядкування бібліографічних описів, побудова таблиць і схеми за авторським текстом, мовно-стилістичне редагування). Постановку задачі, наукові результати та висновки сформульовано авторами самостійно; ШІ не застосовувався для створення основного тексту, оригінальних результатів, статистичного аналізу чи моделювання і не є автором.

Окрема подяка Ткачову Віталію Миколайовичу, помічнику ректора з питань інформаційних технологій Харківського національного університету радіоелектроніки, за те, що саме він створив необхідні умови для реалізації цього проєкту. Без його активної позиції на початковому етапі проведення дослідження було б неможливим.

Дослідження виконано в межах науково-дослідної роботи кафедри комп'ютерного моделювання та інтелектуальних технологій Харківського національного університету радіоелектроніки за темою «Аналіз та захист систем від шкідливого програмного забезпечення».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Верховна Рада України. (2017). Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. https://zakon.rada.gov.ua/go/2163-19
2. Президент України. (2021). Про Стратегію кібербезпеки України: Указ Президента України від 26.08.2021 № 447/2021. https://www.president.gov.ua/documents/4472021-40013
3. Кабінет Міністрів України. (2025). Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності: Постанова Кабінету Міністрів України № 1471. https://zakon.rada.gov.ua/laws/show/1471-2025-п
4. Кабінет Міністрів України. (2025). Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози: Постанова Кабінету Міністрів України № 1533. https://zakon.rada.gov.ua/laws/show/1533-2025-п
5. Кабінет Міністрів України. (2019). Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України № 518. https://zakon.rada.gov.ua/laws/show/518-2019-п
6. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
7. Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST SP 800-61 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3
8. International Organization for Standardization. (2023). ISO/IEC 27035-1:2023 Information technology-Information security incident management-Part 1: Principles and process. ISO/IEC 27035-1:2023
9. International Organization for Standardization. (2023). ISO/IEC 27035-2:2023 Information technology-Information security incident management-Part 2: Guidelines to plan and prepare for incident response. ISO/IEC 27035-2:2023
10. International Organization for Standardization. (2020). ISO/IEC 27035-3:2020 Information technology-Information security incident management-Part 3: Guidelines for ICT incident response operations. ISO/IEC 27035-3:2020
11. International Organization for Standardization. (2024). ISO/IEC 27035-4:2024 Information technology-Information security incident management-Part 4: Coordination. ISO/IEC 27035-4:2024
12. European Union Agency for Cybersecurity. (2020). How to set up CSIRT and SOC: Good practice guide. ENISA. ENISA publication
13. Joint Task Force. (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (NIST SP 800-37 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2
14. Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing (NIST SP 800-150). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-150
15. Schroeder, K., Trinh, H., & Pillitteri, V. (2024). Measurement guide for information security: Volume 1-Identifying and selecting measures (NIST SP 800-55 Vol. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-55v1
16. Schroeder, K., Trinh, H., & Pillitteri, V. (2024). Measurement guide for information security: Volume 2-Developing an information security measurement program (NIST SP 800-55 Vol. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-55v2
17. Cybersecurity and Infrastructure Security Agency. (2020). CISA national cyber incident scoring system (NCISS). CISA National Cyber Incident Scoring System
18. Kertzner, P., Carter, C., & Hahn, A. (2022). Crown jewels analysis for industrial control systems. The MITRE Corporation. MITRE publication
19. Uzlov, D., Yakovlev, S., Tolstoluzka, O., Kopytsia, O., & Burchenko, S. (2025). Integrating CVSS, national criticality levels, and MCDA for multi-factor cyber incident prioritization. Radioelectronic and Computer Systems, 4, 220–235. https://doi.org/10.32620/reks.2025.4.15

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Hennadii Rybachok
Adjunct, Department of Cyber Warfare
National Defence University of Ukraine, Kyiv, Ukraine
ORCID:0009-0002-8513-5133

Serhii Mykus
Doctor of Technical Sciences, Professor,
Deputy Head of the Institute of Information and Communication Technologies and Cyber Defence
National Defence University of Ukraine, Kyiv, Ukraine
ORCID:0000-0002-7103-4166

DECISION FACTORS AND DECISION CONTEXT FOR MILITARY COMMAND AUTHORITIES DURING CYBER INCIDENTS

Abstract. Cyber incident response in the interests of the military command authorities (MCA) of the Armed Forces of Ukraine takes place under time pressure, data incompleteness and mandatory coordination among several subjects of the national response system. For the MCA, the outcome is not the recording of an event's technical indicators but a prepared response decision that defines permitted and prohibited actions, their time windows, priorities and constraints. The current normative framework (Law of Ukraine No. 2163-VIII, the Cybersecurity Strategy of Ukraine, Resolutions of the Cabinet of Ministers of Ukraine No. 1471 and No. 1533 of November 2025) and international process models (NIST CSF 2.0, NIST SP 800-61 Rev. 3, the ISO/IEC 27035 series) regulate the response sequence in detail but do not treat the conditions of decision-making as a distinct object of description. As a result, different units may rely on divergent assumptions about constraints, priorities and consequences, which reduces the comparability of decisions even for technically similar incidents. The paper proposes a taxonomy of internal and external factors influencing decisions and a structure of the decision context as a consistent input-data package decomposed into mission context, policy constraints, asset context and threat intelligence. To reduce uncertainty, a status attribute (known, assumed, unknown) and artefact-based confirmation of key parameters are introduced, and traceability is supported by a role framework of subjects who form and approve context elements. A correspondence matrix "factor – context element – decision consequence" and a minimal artefact checklist are constructed as a practical instrument for preparing a decision within the response loop. The results separate the incident description from the decision-making conditions, improve the comparability of decisions for typical incident classes and form a terminological and conceptual basis for the subsequent justification of an assessment system of indicators and criteria. The proposed apparatus does not duplicate prioritization or alternative-selection models but precedes them by fixing the input conditions on which such models rely.

Keywords: cyber incident; military command authorities; decision-making; decision context; decision factors; response loop; artefact; threat intelligence; critical infrastructure.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Verkhovna Rada of Ukraine. (2017). *On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII dated October 5, 2017*. https://zakon.rada.gov.ua/go/2163-19
2. President of Ukraine. (2021). *On the Cybersecurity Strategy of Ukraine: Decree of the President of Ukraine No. 447/2021 dated August 26, 2021*. https://www.president.gov.ua/documents/4472021-40013
3. Cabinet of Ministers of Ukraine. (2025). *On approval of the procedure for interaction between entities of the national cyber incident, cyberattack, and cyberthreat response system and entities responsible for cybersecurity, law enforcement, counterintelligence and intelligence agencies, and entities carrying out operational-search activities: Resolution of the Cabinet of Ministers of Ukraine No. 1471*. https://zakon.rada.gov.ua/laws/show/1471-2025-п
4. Cabinet of Ministers of Ukraine. (2025). *Certain issues of responding to cyber incidents, cyberattacks, and cyberthreats: Resolution of the Cabinet of Ministers of Ukraine No. 1533*. https://zakon.rada.gov.ua/laws/show/1533-2025-п

5. Cabinet of Ministers of Ukraine. (2019). *On approval of the general requirements for cyber protection of critical infrastructure facilities: Resolution of the Cabinet of Ministers of Ukraine No. 518*. https://zakon.rada.gov.ua/laws/show/518-2019-п
6. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
7. Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST SP 800-61 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3
8. International Organization for Standardization. (2023). *Information technology—Information security incident management—Part 1: Principles and process* (ISO/IEC Standard No. 27035-1:2023).
9. International Organization for Standardization. (2023). *Information technology—Information security incident management—Part 2: Guidelines to plan and prepare for incident response* (ISO/IEC Standard No. 27035-2:2023).
10. International Organization for Standardization. (2020). *Information technology—Information security incident management—Part 3: Guidelines for ICT incident response operations* (ISO/IEC Standard No. 27035-3:2020).
11. International Organization for Standardization. (2024). *Information technology—Information security incident management—Part 4: Coordination* (ISO/IEC Standard No. 27035-4:2024).
12. European Union Agency for Cybersecurity. (2020). *How to set up CSIRT and SOC: Good practice guide*. ENISA.
13. Joint Task Force. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (NIST SP 800-37 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2
14. Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). *Guide to cyber threat information sharing* (NIST SP 800-150). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-150
15. Schroeder, K., Trinh, H., & Pillitteri, V. (2024). *Measurement guide for information security: Volume 1—Identifying and selecting measures* (NIST SP 800-55 Vol. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-55v1
16. Schroeder, K., Trinh, H., & Pillitteri, V. (2024). *Measurement guide for information security: Volume 2—Developing an information security measurement program* (NIST SP 800-55 Vol. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-55v2
17. Cybersecurity and Infrastructure Security Agency. (2020). *CISA national cyber incident scoring system (NCISS)*.
18. Kertzner, P., Carter, C., & Hahn, A. (2022). *Crown jewels analysis for industrial control systems*. The MITRE Corporation.
19. Uzlov, D., Yakovlev, S., Tolstoluzka, O., Kopytsia, O., & Burchenko, S. (2025). Integrating CVSS, national criticality levels, and MCDA for multi-factor cyber incident prioritization. *Radioelectronic and Computer Systems*, *4*, 220–235. https://doi.org/10.32620/reks.2025.4.15

Отримано редакцією журналу / Received: 28.01.26
Прорецензовано / Revised: 08.02.26
Схвалено до друку / Accepted: 24.09.26