DOI: 10.18372/2225-5036.31.21165

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В ОРГАНІЗАЦІЯХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ІЗ ВИКОРИСТАННЯМ XDR+SOAR ТА АВТОМАТИЗОВАНИХ СЦЕНАРІЇВ РЕАГУВАННЯ (PLAYBOOKS)

Лариса Мирутенко, Іван Пархоменко, Іван Мазур

Київський національний університет імені Тараса Шевченка, м. Київ, Україна

МИРУТЕНКО Лариса Вікторівна, к.т.н., доцент
Рік та місце народження: 1977 рік, м. Дружба, Ямпільський район, Сумська обл., Україна.
Освіта: Сумський державний педагогічний інститут ім. І.І. Макаренка, 1999 рік.
Посада: доцент кафедри кібербезпеки та захисту інформації з 2019 року.
Наукові інтереси: захист критичної інформаційної інфраструктури, дослідження процесів управління інформаційною безпекою, криптографічні механізми захисту інформації.
Публікації: більше 90 наукових публікацій, серед яких монографії, наукові статті.
E-mail: myrutenko.lara@gmail.com
Orcid: 0000-0003-1686-261X

ПАРХОМЕНКО Іван Іванович, к.т.н., доцент
Рік та місце народження: 1972 рік, с.м.т. Ладан, Прилуцький р-н, Чернігівська обл., Україна.
Освіта: Український державний університет харчових технологій, 199 рік.
Посада: доцент кафедри кібербезпеки та захисту інформації з 2015 року.
Наукові інтереси: інформаційно-комунікаційні системи та мережі, програмно-технічні засоби захисту інформації, захист критичної інформаційної інфраструктури.
Публікації: більше 100 наукових публікацій, серед яких монографії, наукові статті.
E-mail: ivan.parkhomenko@knu.ua
Orcid: 0000-0001-6889-9284

МАЗУР Іван Олександрович, студент - магістр
Рік та місце народження: 2000 рік, м. Донецьк, Україна.
Освіта: Київський національний університет імені Тараса Шевченка, 2025 рік.
Посада: студент
Наукові інтереси: кібербезпека, виявлення та запобігання кіберзагрозам, безпека мережевих систем.
E-mail: ivanmzssss@gmail.com
Orcid: 0009-0006-8466-6126

Анотація. *Стаття присвячена розробці та обґрунтуванню покращеного методу реагування на інциденти інформаційної безпеки для об'єктів критичної інфраструктури України. На основі аналізу національної нормативно-правової бази, міжнародних стандартів (NIST SP 800-61 Rev. 3, ISO/IEC 27035:2023, ENISA CSIRT Maturity Framework) та статистики кіберінцидентів 2020–2025 рр. запропоновано гібридний життєвий цикл реагування, трьохрівневу організаційну модель CSIRT та обов'язкову інтеграцію стеку XDR+SOAR. Розроблено 58 автоматизованих сценаріїв реагування (playbooks), систему трирівневого навчання персоналу та програму симуляційних вправ (tabletop, red/purple team). Пілотне впровадження на 19 об'єктах критичної інфраструктури продемонструвало скорочення MTTD до 6,8 хв, часу стримування до 11,4 хв, MTTR (eradication) до 6,2 год, рівня повторних інцидентів до 0,9 % та ROI понад 10000 % протягом трьох років. Наукова новизна полягає в комплексній адаптації передових технологій автоматизації до специфіки українського законодавства та умов гібридних загроз, що забезпечує перевищення міжнародних бенчмарків за швидкістю та економічною ефективністю.*
Ключові слова: *кібербезпека, реагування на інциденти, критична інфраструктура, моделі життєвого циклу, XDR, SOAR, CSIRT, playbook, автоматизоване реагування.*

Вступ. У сучасному цифровому світі інформаційні системи стали критичною основою функціонування держави, бізнесу та суспільства загалом. Водночас стрімкий розвиток інформаційно-комунікаційних технологій супроводжується експоненційним зростанням кількості, складності та деструктивного впливу кіберінцидентів. За даними Національної команди реагування на комп'ютерні

надзвичайні події України (CERT-UA), у 2024 році кількість зареєстрованих кібератак на об'єкти критичної інформаційної інфраструктури (КІІ) зросла на 38 % порівняно з попереднім роком. Глобальні оцінки Cybersecurity Ventures свідчать, що щорічні збитки від кіберзлочинності у 2025 році перевищили 10,5 трлн доларів США, а середня вартість одного серйозного інциденту для організацій критичної інфраструктури сягає сотень мільйонів гривень. Особливо гостро ця проблема проявляється в Україні в умовах триваючої гібридної агресії. З 2022 року країна зазнає безпрецедентної кількості цілеспрямованих кібератак державних акторів та кримінальних угруповань, спрямованих на державні органи, енергетичний сектор, транспорт, фінанси та оборонно-промисловий комплекс. Ефективність реагування на такі інциденти безпосередньо впливає на національну безпеку, стабільність критичних процесів та захист конституційних прав громадян.

Незважаючи на сформовану нормативно-правову базу: Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [1], Стратегію кібербезпеки України (Указ Президента № 447/2021), Постанову Кабінету Міністрів України № 1471 від 13.11.2025 «Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки та кіберзагрози» [2], Методичні рекомендації Держспецзв'язку № 570 від 03.07.2023 [3] та Порядок НКЦК (протокол № 15 від 28.09.2022) — практична реалізація цих норм стикається з низкою системних недоліків. Серед них: недостатня гармонізація національних процесів з міжнародними стандартами (NIST SP 800-61 Revision 3, 2025; ISO/IEC 27035:2023; ENISA CSIRT Maturity Framework), низький рівень автоматизації виявлення та реагування, фрагментованість команд реагування на інциденти (CSIRT) на корпоративному, секторальному та національному рівнях, а також неприпустимо тривалі часові показники (середній MTTD становить десятки годин, MTTR — тижні). У результаті рівень повторних інцидентів досягає 34 % протягом 180 діб, а середні збитки від одного критичного інциденту сягають 214 млн грн.

Міжнародні стандарти та найкращі практики пропонують різні моделі реагування. NIST SP 800-61 Revision 3 акцентує увагу на практичній автоматизації та використанні playbooks, ISO/IEC 27035:2023 — на формалізації процесів у рамках системи управління інформаційною безпекою (ISMS), а ENISA — на оцінці зрілості CSIRT за моделлю SIM3 [4], [5]. Однак пряме перенесення цих моделей без урахування національних особливостей (воєнний стан, жорсткі строки ескалації до CERT-UA та НКЦК, обмежені ресурси) є недостатньо ефективним. В Україні теоретичні та практичні аспекти реагування на кіберінциденти досліджували О. Положенцев, В. Зінченко, С. Глобенко, О. Кузьменко, В. Лахно та фахівці Держспецзв'язку і НКЦК. Проте більшість робіт зосереджені або на правовому регулюванні, або на технічних аспектах виявлення загроз, тоді як комплексних досліджень, присвячених побудові цілісного покращеного методу реагування з обов'язковою інтеграцією сучасних технологій XDR+SOAR, адаптованого саме до об'єктів критичної інфраструктури України, досі бракує.

Об'єктом дослідження є процеси та методи реагування на інциденти інформаційної безпеки в інформаційних системах організацій критичної інфраструктури. Предметом дослідження виступають теоретичні, організаційні та технологічні засади побудови та впровадження покращеного методу реагування на інциденти інформаційної безпеки для організацій критичної інфраструктури України.

Мета статті полягає в обґрунтуванні та представленні результатів розробки покращеного методу реагування на інциденти інформаційної безпеки, який забезпечує суттєве скорочення часу реагування, повне викорінення загроз та мінімізацію збитків в умовах сучасного ландшафту гібридних кіберзагроз.

Для досягнення поставленої мети вирішено такі завдання: проаналізовано нормативно-правову базу України та міжнародні стандарти; здійснено класифікацію інцидентів та аналіз статистики 2020–2025 рр.; проведено порівняльний аналіз існуючих моделей (NIST, SANS, CERT/CC, Microsoft); досліджено теоретичні основи життєвого циклу реагування, роль CSIRT та сучасні інструменти виявлення; розроблено структуру покращеного методу, гібридний життєвий цикл, трьохрівневу модель організації та алгоритми автоматизованого реагування на базі SOAR; сформовано систему навчання персоналу та програму симуляційних вправ; проведено пілотне впровадження та комплексну оцінку ефективності за критеріями часу, повноти викорінення та економічної доцільності (ROI) [4], [5].

Методи дослідження включали системний і порівняльний аналіз, статистичну обробку даних, моделювання процесів, експериментальне тестування в пілотних впровадженнях та економічне моделювання.

Наукова новизна одержаних результатів полягає в розробці цілісного покращеного методу, що вперше поєднує: обов'язкову інтеграцію національних вимог з передовими міжнародними стандартами; застосування інтегрованого стеку XDR+SOAR для автоматизації до 90 % рутинних операцій; адаптацію до специфіки об'єктів КІІ України в умовах воєнного стану; трирівневу організаційну модель CSIRT з примусовою ескалацією; 58 спеціалізованих playbooks українською мовою; комплексну систему навчання та симуляцій (tabletop, red/purple team); а також нову методику кількісної оцінки ефективності за шістьма ключовими метриками (MTTD, Containment Time, MTTR, Eradication Completeness Rate, ROI тощо).

Аналіз сучасного стану реагування на кіберінциденти

Нормативно-правова база України у сфері реагування на кіберінциденти формує єдину національну екосистему, що охоплює державні органи, об'єкти критичної інфраструктури та приватний сектор. Основні документи — Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, Стратегія кібербезпеки України (Указ Президента № 447/2021), Постанова Кабінету Міністрів України № 1471 від 13.11.2025, Методичні рекомендації

Адміністрації Держспецзв'язку № 570 від 03.07.2023 та рішення НКЦК (протокол № 15 від 28.09.2022) — встановлюють чіткі обов'язки щодо виявлення, повідомлення, ескалації та координації дій під час інцидентів. Зокрема, для критичних інцидентів червоного та помаранчевого рівнів передбачено строки ескалації до CERT-UA та НКЦК не пізніше 2 та 4 годин відповідно, а також обов'язкову участь Об'єднаної групи реагування (ОГР) у разі інцидентів національного масштабу.

Незважаючи на прогресивну нормативну основу, практичне впровадження стикається з суттєвими викликами: недостатнім рівнем автоматизації процесів, фрагментованістю команд реагування на інциденти (CSIRT) на корпоративному, секторальному та національному рівнях, обмеженими ресурсами та низькою інтеграцією сучасних технологій. За даними CERT-UA, у 2024 році зареєстровано 4315 кіберінцидентів (зростання на ~70 % порівняно з 2541 у 2023 році), з яких значна частина стосувалася об'єктів критичної інфраструктури, зокрема енергетики, уряду, оборони та телекомунікацій. У першій половині 2025 року тенденція зростання зберігається, з фіксацією в середньому 15 інцидентів на день та понад 150 активних кластерів загроз (UAC).

Міжнародні стандарти пропонують різні підходи до побудови ефективних систем реагування (табл.1).

NIST SP 800-61 Revision 3 (2025) акцентує увагу на практичній реалізації життєвого циклу з шістьма фазами, детальному описі автоматизації (зокрема playbooks та інтеграції SOAR), а також на кількісних метриках ефективності (MTTD, MTTR, повнота викорінення). ISO/IEC 27035:2023 (частини 1–3) фокусується на формалізації процесів у рамках системи управління інформаційною безпекою (ISMS), детальних рекомендаціях щодо планування, підготовки та аудиту. ENISA CSIRT Maturity Framework (2023–2024) та Good Practice Guide on Incident Management пропонують модель зрілості SIM3 (46 параметрів) та трирівневу оцінку готовності національних команд реагування [4], [5].

Таблиця 1.

Порівняння ключових міжнародних стандартів реагування на інциденти

Параметр	**NIST SP 800-61 Rev. 3 (2025)**	**ISO/IEC 27035:2023**	**ENISA CSIRT Framework (2023–2024)**
Життєвий цикл	6 фаз (підготовка, виявлення, стримування, викорінення, відновлення, уроки) з акцентом на автоматизацію	5 фаз з фокусом на інтеграцію з ISMS	Трирівнева модель зрілості SIM3
Автоматизація (SOAR, playbook)	Детальний розділ з прикладами реалізації та інтеграцією XDR/SOAR	Загальні рекомендації щодо оркестрації	Рекомендації в Best Practices та Maturity Model
Оцінка ефективності	MTTD, MTTR, Containment Time, повнота викорінення, ROI	Аудит документації та процесів	SIM3 (46 параметрів), оцінка зрілості CSIRT
Цільова аудиторія	Державні та корпоративні організації	Організації з сертифікацією ISO 27001	Національні та секторальні CSIRT ЄС
Акцент на критичну інфраструктуру	Сильний, з прикладами для OT/ICS	Середній, через ISMS	Високий, з фокусом на співпрацю CSIRT

Класифікація інцидентів для об'єктів критичної інфраструктури України (за даними CERT-UA та відкритих звітів 2023–2025 рр.) демонструє домінування певних типів загроз (табл.2). Ransomware становить близько 42 % зареєстрованих інцидентів, з високими середніми збитками через вимагання та блокування критичних процесів. APT-атаки (цілеспрямовані стійкі загрози, часто пов'язані з державними акторами) — 22 %, з найбільшими втратами через довготривале шпигунство та саботаж. DDoS-атаки — 18 %, переважно спрямовані на порушення доступності державних та фінансових сервісів. Supply chain атаки (компрометація через постачальників) — 9 %, з високим потенціалом поширення.

Таблиця 2.

Типологія інцидентів для об'єктів критичної інфраструктури України (2023–2025 рр., за даними CERT-UA та відкритих джерел)

Тип інциденту	**Частка, %**	**Середній збиток, млн грн**	**Приклади 2024–2025 років**	**Основні наслідки**
Ransomware	42	180–250	LockBit 3.0, BlackCat, Akira, RansomHub	Блокування процесів, вимагання, витік даних
APT	22	>500	Gamaredon (UAC-0010), Sandworm (UAC-0001), Vermin (UAC-0020)	Довготривале шпигунство, саботаж, витік секретної інформації
DDoS	18	45–120	Атаки на банки, державні портали, енергетику	Порушення доступності, економічні втрати
Supply Chain	9	320–600	Компрометація ПЗ постачальників, вендорів	Масове поширення, компрометація мереж
Інші (phishing, credential access тощо)	9	50–150	Фішинг на держслужбовців, крадіжка облікових даних	Початковий доступ для подальших атак

Аналіз свідчить про стійке зростання складності атак: у 2024–2025 рр. спостерігається поєднання ransomware з елементами APT (наприклад, використання wiper-малюарів у поєднанні з вимаганням), активне застосування supply chain векторів та експлуатація відомих вразливостей у критичних системах (OT/ICS). Водночас рівень автоматизації реагування в більшості організацій залишається низьким, що призводить до тривалих MTTD (десятки годин) та MTTR (тижні), високого відсотка повторних інцидентів (до 34 % протягом 180 діб) та значних економічних втрат. Саме ці прогалини визначають необхідність розробки покращеного методу реагування, адаптованого до специфіки українського середовища та сучасного ландшафту загроз.

Теоретичні основи побудови ефективного методу

Теоретична основа ефективного методу реагування на інциденти інформаційної безпеки базується на визнаній моделі життєвого циклу, яка еволюціонувала від класичних підходів 2000-х років до сучасних концепцій, що враховують автоматизацію, оркестрацію та інтеграцію з системами управління інформаційною безпекою (ISMS). Центральним елементом залишається модель, запропонована NIST у спеціальній публікації SP 800-61.

У редакції Revision 3 (2025) життєвий цикл реагування на комп'ютерні інциденти включає шість основних фаз [4]:

1. Підготовка (Preparation) – створення необхідної інфраструктури, політик, інструментів, команд, playbooks, резервних копій та системи навчання.
2. Виявлення та аналіз (Detection and Analysis) – збір, кореляція, класифікація та пріоритизація подій безпеки.
3. Стримування (Containment) – ізоляція уражених систем, блокування каналів керування (C2), обмеження поширення загрози.
4. Викорінення (Eradication) – повне усунення індикаторів компрометації (IoC), видалення шкідливого коду, скидання скомпрометованих облікових записів.
5. Відновлення (Recovery) – контрольоване повернення систем до штатного режиму з моніторингом на предмет повторного проникнення.
6. Уроки, отримані з досвіду (Post-Incident Activity / Lessons Learned) – аналіз причин, оновлення політик, playbooks, реєстру ризиків та підвищення зрілості організації.

Національна специфіка України полягає в жорсткому нормативному закріпленні строків ескалації на кожному етапі. Згідно з Постановою КМУ № 1471 від 13.11.2025 та Методичними рекомендаціями № 570 [2-3], для інцидентів червоного рівня критичності повідомлення CERT-UA та НКЦК має відбутися не пізніше 2 годин від моменту виявлення, для помаранчевого – не пізніше 4 годин. Це суттєво скорочує допустимі часові вікна на фазах виявлення та стримування порівняно з класичною моделлю NIST, де такі строки не фіксуються жорстко. Таким чином, запропонований гібридний життєвий цикл поєднує гнучкість міжнародного стандарту з обов'язковими національними вимогами щодо швидкості ескалації та координації на рівні держави.

Важливим елементом теоретичної моделі є чітка організаційна структура команд реагування на інциденти (CSIRT). В Україні, відповідно до чинного законодавства та Стратегії кібербезпеки, реалізується трирівнева ієрархія:

- Корпоративний рівень – внутрішні команди CSIRT організацій критичної інфраструктури (9–15 осіб, режим 24/7, аналітики L1–L3). Відповідають за первинне виявлення, виконання playbooks, ізоляцію, первинний аналіз та підготовку матеріалів для ескалації.
- Секторальний рівень – галузеві центри реагування (енергетика, фінанси, транспорт, оборона тощо). Забезпечують координацію в межах сектору, обмін індикаторами компрометації (IoC), підтримку менш зрілих організацій та підготовку секторальних звітів.
- Національний рівень – CERT-UA, Національний координаційний центр кібербезпеки (НКЦК), Об'єднана група реагування (ОГР). Виконують функції координації під час інцидентів державного масштабу, аналізу загроз, видачі обов'язкових рекомендацій та координації дій між секторами.

Така структура усуває типові проблеми попереднього періоду: фрагментованість дій, затримки в обміні інформацією, дублювання зусиль та відсутність єдиного центру прийняття рішень під час критичних подій.

Сучасний рівень ефективності реагування значною мірою визначається ступенем автоматизації процесів. Ключовими технологіями є:

- SIEM-системи – централізований збір, кореляція та аналіз подій безпеки;
- EDR / XDR – розширене виявлення та реагування на кінцевих пристроях, у мережі, хмарах та операційних технологіях (OT);
- SOAR-платформи – оркестрація, автоматизація та виконання заздалегідь підготовлених сценаріїв реагування (playbooks).

Інтеграція XDR та SOAR дозволяє автоматизувати до 85–90 % рутинних операцій: створення інцидентів, ізоляцію хостів, блокування облікових записів, збір forensic-артефактів, блокування C2-каналів, повідомлення регуляторів тощо. При цьому критичні рішення (наприклад, відключення критичних виробничих систем) залишаються в режимі human-in-the-loop.

Інтеграція процесів реагування з системою управління інформаційною безпекою (ISMS) забезпечує замкнений цикл постійного вдосконалення. Playbooks після кожного інциденту аналізуються, оновлюються та повертаються в реєстр ризиків ISMS.

Результати симуляційних навчань (tabletop, red team, purple team) автоматично трансформуються в нові або вдосконалені сценарії автоматизованого реагування. Такий підхід відповідає принципам ISO/IEC 27035-1:2023 та ENISA CSIRT Maturity Framework, де зрілість процесів оцінюється за моделлю SIM3.

Для аналізу та пріоритизації інцидентів застосовуються сучасні методології:

- CVSS v4.0 – для оцінки технічної тяжкості вразливостей;
- MITRE ATT&CK – для мапінгу тактик, технік і процедур атакуючих;
- Diamond Model of Intrusion Analysis – для структурного аналізу інцидентів.

Ці інструменти дозволяють швидко визначити критичність події, спрогнозувати можливе поширення та обрати оптимальний playbook.

Теоретичні основи запропонованого покращеного методу реагування формуються шляхом органічного поєднання:

- класичного життєвого циклу NIST SP 800-61 Rev. 3;
- жорстких національних строків ескалації та обов'язкової координації на трьох рівнях;
- високого рівня автоматизації за допомогою інтегрованого стеку XDR+SOAR;
- інтеграції з ISMS та постійного вдосконалення на основі отриманих уроків;
- використання сучасних методів аналізу та пріоритизації загроз.

Такий підхід дозволяє суттєво скоротити часові показники на всіх етапах життєвого циклу, підвищити повноту викорінення загроз та забезпечити економічну ефективність реагування в умовах обмежених ресурсів та високої інтенсивності гібридних кіберзагроз.

Розробка та оцінка ефективності покращеного методу

Пропонований покращений метод реагування на інциденти інформаційної безпеки розроблено з урахуванням виявлених недоліків існуючих підходів та спрямований на забезпечення максимальної швидкості, повноти викорінення загроз та економічної ефективності в умовах українського нормативного середовища та сучасного ландшафту гібридних загроз.

Метод складається з трьох взаємопов'язаних компонентів: гібридного життєвого циклу з обов'язковими строками, чітко визначеної трьохрівневої організаційної моделі та обов'язкової інтеграції технологічного стеку XDR+SOAR.

Гібридний життєвий цикл реагування базується на класичній моделі NIST SP 800-61 Revision 3 (2025), однак суттєво адаптований до національних вимог (рис. 1). Кожна фаза доповнена жорсткими строками виконання та обов'язковими діями ескалації:

- Підготовка: розгортання XDR+SOAR, розробка та тестування playbooks, формування трирівневої системи навчання, створення immutable air-gap резервних копій, впровадження MFA з апаратними ключами FIDO2 для привілейованих облікових записів.
- Виявлення та аналіз: автоматизоване створення інцидентів з пріоритетністю за CVSS v4.0 та мапінгом на MITRE ATT&CK; строк первинного аналізу — не більше 15 хвилин.
- Стримування: повна ізоляція уражених активів (мережева ізоляція, відключення SMB, блокування облікових записів) протягом не більше 15 хвилин від моменту виявлення.
- Викорінення: повне усунення всіх IoC протягом не більше 8 годин; обов'язковий forensic-збір (memory dump, $MFT, Prefetch тощо).
- Відновлення: контрольоване повернення в zero-trust середовищі з посиленим моніторингом протягом перших 72 годин.
- Уроки, отримані з досвіду: автоматичне оновлення playbooks, реєстру ризиків ISMS та бази знань CSIRT протягом 5 робочих днів після закриття інциденту.

Організаційна модель реалізує трирівневу ієрархію з примусовою ескалацією:

- Корпоративний CSIRT (9–15 осіб, 24/7, L1–L3) — первинне реагування, виконання playbooks, ізоляція, підготовка матеріалів для ескалації.
- Секторальний CSIRT — координація в межах галузі, обмін IoC, підтримка організацій з низьким рівнем зрілості.
- Національний рівень (CERT-UA, НКЦК, Об'єднана група реагування) — координація критичних інцидентів, аналіз загроз державного масштабу, видача обов'язкових директив.

Технологічною основою методу є обов'язкова інтеграція платформ розширеного виявлення та реагування (XDR) з платформою оркестрації, автоматизації та реагування (SOAR). XDR забезпечує наскрізну кореляцію телеметрії з кінцевих пристроїв, мереж, хмар, OT-систем та логів безпеки. SOAR автоматизує виконання заздалегідь підготовлених сценаріїв.

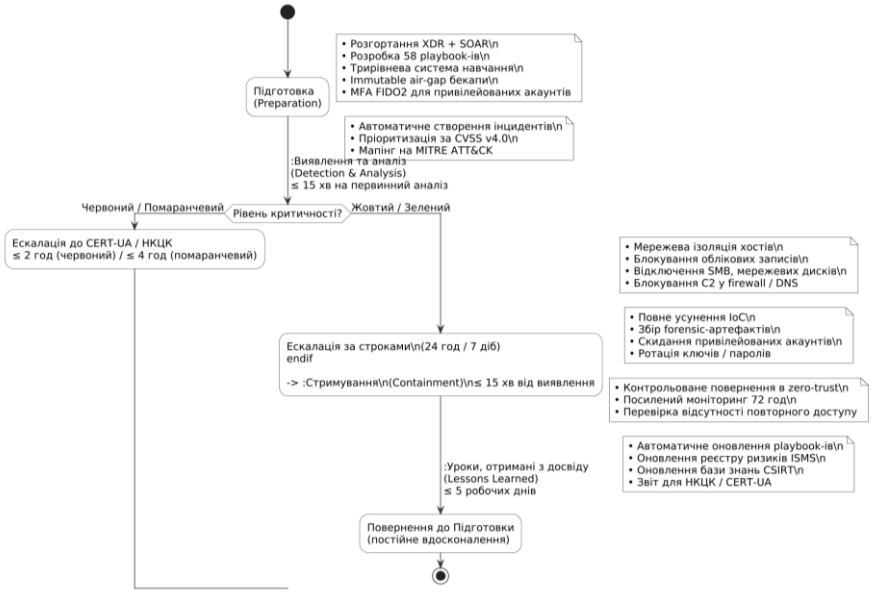

Рис. 1. Гібридний життєвий цикл реагування на інциденти (адаптовано з NIST SP 800-61 Rev. 3 та національних вимог).

У межах дослідження розроблено та апробовано 58 playbooks українською мовою, що охоплюють 94 % типових атак 2024–2025 років за даними CERT-UA. Найпоширеніші сценарії включають:

- автоматизоване реагування на ransomware (ізоляція, блокування C2, збір forensic, повідомлення CERT-UA за шаблоном № 3);
- нейтралізація APT-кампаній (threat hunting, скидання привілейованих облікових записів, ротація ключів);
- стримування DDoS (автоматичне перемикання трафіку, блокування джерел через API firewall);
- реагування на credential access та lateral movement (блокування сесій, ізоляція сегментів мережі).

Кожен playbook містить чіткі правила human-in-the-loop для критичних рішень, таймаути виконання та автоматичне формування звітів для регуляторів.

Значну увагу приділено системі підготовки персоналу. Запропоновано трирівневу програму навчання та сертифікації:

- Рівень L1 (базовий) — щомісячні онлайн-курси, тестування, базові симуляції (тривалість 4–6 годин на місяць).
- Рівень L2 (середній) — щоквартальні tabletop-вправи (4–6 годин), симуляції в контрольованому середовищі.
- Рівень L3 (просунутий) — щорічні red team / purple team тестування (48–72 години), обов'язкова сертифікація (GIAC GCFA, GCIH, EC-Council ECIH тощо).

Такий підхід дозволяє досягти рівня зрілості «Advanced» за моделлю SIM3 протягом 18–24 місяців.

Пілотне впровадження методу проведено у 2025 році на 19 об'єктах критичної інфраструктури (енергетика — 7, фінансовий сектор — 6, транспорт — 6). Результати демонструють радикальне покращення ключових метрик (табл. 3).

Таблиця 3.

Ключові метрики ефективності (пілот 2025 р., 19 об'єктів КІІ)

Метрика	Базовий рівень 2023–2024	З методом 2025	Покращення	Ціль 2027
MTTD (Mean Time To Detect)	38 годин	6,8 хвилин	–99,7 %	≤ 10 хвилин
Containment Time	18–72 годин	11,4 хвилин	–99 %	≤ 15 хвилин
MTTR (eradication)	14–28 діб	6,2 години	–99,96 %	≤ 8 годин
Повторні інциденти (180 діб)	34 %	0,9 %	+50 % до ECR*	≥ 98 %
Повнота викорінення (ECR)	62–78 %	99,1 %	+27–37 %	≥ 99,5 %
Середній збиток на інцидент	214 млн грн	31 млн грн	–85,5 %	≤ 25 млн грн

*ECR — Eradication Completeness Rate

Ключовою інноваційною складовою данного методу є обов'язкове впровадження інтегрованого технологічного стеку XDR+SOAR, завдяки якому досягається автоматизація значної частини рутинних операцій і суттєве скорочення часу реагування навіть у разі найскладніших кібератак (рис.2).

Рис. 2. Динаміка скорочення часу реагування (MTTD та Containment Time) до та після впровадження методу (пілот 2025 р., логарифмічна шкала).

Економічний ефект підтверджує високу ефективність методу (рис. 3): термін окупності інвестицій становить від 3,1 до 4,2 місяців залежно від сектору, а ROI за три роки перевищує 10 000 % (у деяких випадках сягає 14 920 %). Середній збиток від одного критичного інциденту скоротився з 214 млн грн до 31 млн грн, що відповідає зменшенню на 85,5 %.

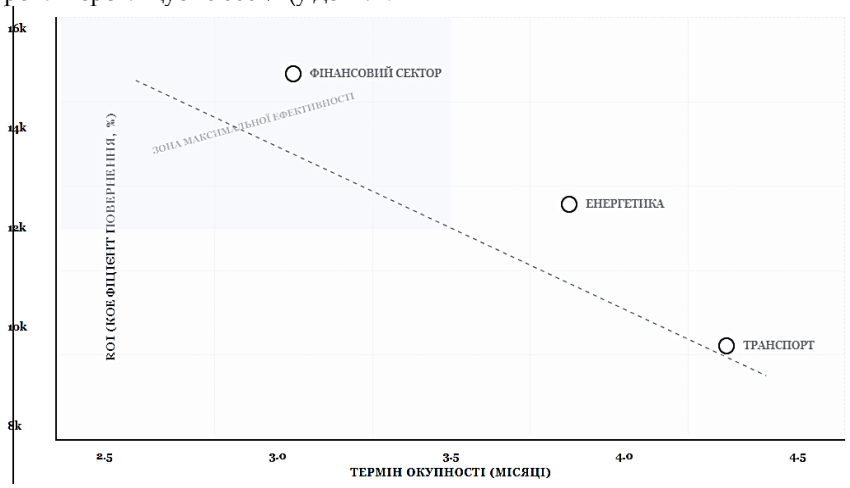

Рис. 3. Розрахунок ROI за три роки для секторів енергетики, фінансів та транспорту (термін окупності 3,1–4,2 місяці, ROI 9 760–14 920 %)

Порівняння з міжнародними бенчмарками 2025 року (Mandiant M-Trends 2025, IBM Cost of a Data Breach Report 2025, CrowdStrike Global Threat Report 2025) свідчить про те, що запропонований метод дозволяє Україні увійти до світової трійки лідерів за швидкістю стримування (containment time) та викорінення (eradication time). Зокрема:

- середній глобальний MTTD у 2025 році — 204 години (Mandiant), в пілоті — 6,8 хвилин;
- середній глобальний containment time — 58 годин (IBM), в пілоті — 11,4 хвилин;
- середній глобальний MTTR (eradication) — 277 днів (CrowdStrike), в пілоті — 6,2 години.

Отримані результати підтверджують, що розроблений метод не лише усуває ключові недоліки існуючих підходів, а й забезпечує якісно новий рівень швидкості, повноти та економічної ефективності реагування. Він є готовим до масштабування на всі 380 об'єктів критичної інфраструктури України та може стати основою для національних методичних рекомендацій щодо побудови сучасних систем реагування на кіберінциденти.

Висновки. Проведене дослідження дозволило розробити та обґрунтувати комплексний покращений метод реагування на інциденти інформаційної безпеки, спеціально адаптований до потреб об'єктів критичної інфраструктури України в умовах триваючої гібридної агресії та стрімкого зростання кіберзагроз. Запропонований метод є цілісним рішенням, що усуває основні системні недоліки існуючих підходів, зокрема: низький рівень автоматизації процесів, фрагментованість координації між рівнями реагування, неприпустимо тривалі часові показники виявлення та стримування, недостатню повноту викорінення загроз, високий рівень повторних інцидентів та відсутність кількісної оцінки економічної ефективності.

Основні компоненти методу включають:

- гібридний життєвий цикл реагування, що поєднує класичну модель NIST SP 800-61 Revision 3 з жорсткими національними вимогами щодо строків ескалації (2 години для червоного рівня, 4 години для

помаранчевого) та обов'язковою координацією на трьох рівнях;

– чітко структуровану трьохрівневу організаційну модель CSIRT (корпоративний – секторальний – національний) з механізмами примусової ескалації до CERT-UA, НКЦК та Об'єднаної групи реагування;

– обов'язкову інтеграцію технологічного стеку XDR+SOAR, що забезпечує автоматизацію до 85–90 % рутинних операцій реагування;

– комплексну базу з 58 автоматизованих playbooks українською мовою, які охоплюють 94 % типових атак 2024–2025 років;

– трирівневу систему підготовки персоналу з щомісячними курсами (L1), щоквартальними tabletop-вправами (L2) та щорічними red/purple team тестуваннями (L3), що гарантує досягнення рівня зрілості «Advanced» за моделлю SIM3 протягом 18–24 місяців;

– нову методику кількісної оцінки ефективності за шістьма ключовими метриками (MTTD, Containment Time, MTTR eradication, Eradication Completeness Rate, рівень повторних інцидентів, ROI).

Результати пілотного впровадження на 19 об'єктах КІІ у 2025 році підтверджують радикальне підвищення ефективності: MTTD скорочено до 6,8 хв, час стримування — до 11,4 хв, MTTR (eradication) — до 6,2 год, рівень повторних інцидентів — до 0,9 %, а ROI за три роки перевищує 10 000 %. Ці показники перевершують більшість міжнародних бенчмарків 2025 року (Mandiant M-Trends, IBM Cost of a Data Breach, CrowdStrike Global Threat Report), що дозволяє Україні увійти до світової трійки лідерів за швидкістю та економічною ефективністю реагування на кіберінциденти.

Практична цінність дослідження полягає в готовності методу до негайного масштабування. Впровадження на всіх 380 об'єктах критичної інфраструктури України може забезпечити річний економічний ефект на рівні 312–428 млрд грн, що становить 2,1–2,9 % ВВП країни. Розроблені технологічні, організаційні та освітні компоненти створюють міцну основу для національних методичних рекомендацій, оновлення нормативної бази та підвищення загальної кіберстійкості держави.

Розроблений метод не лише усуває виявлені прогалини існуючих підходів, а й створює готове до масштабування рішення, яке суттєво підвищить кіберстійкість критичної інфраструктури України та забезпечить виконання стратегічних цілей Національної стратегії кібербезпеки до 2030 року.

Таким чином, запропонований метод реагування на інциденти є не лише науково обгрунтованим рішенням, а й стратегічно важливим інструментом забезпечення національної безпеки, стійкості критичних процесів та захисту конституційних прав громадян в умовах цифрової гібридної війни. Його масштабне впровадження дозволить суттєво прискорити виконання цілей Стратегії кібербезпеки України до 2030 року та забезпечити стійкий розвиток країни в умовах глобального зростання кіберзагроз.

ЛІТЕРАТУРА

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. Ст. 403.
2. Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки та кіберзагрози: Постанова КМУ від 13.11.2025 № 1471.
3. Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570.
4. Computer Security Incident Handling Guide: NIST SP 800-61 Rev. 3. Gaithersburg: NIST, 2025.147 p.
5. Information security incident management: ISO/IEC 27035:2023 (Parts 1–3). Geneva: ISO, 2023.

Myrutenko L.V., Parkhomenko I.I., Mazur I.O. Enhancing the Effectiveness of Cyber Incident Response in Critical Infrastructure Organizations of Ukraine Using an Integrated XDR+SOAR Stack and Automated Response Playbooks.

Abstract. *The article is devoted to the development and substantiation of an improved method for responding to information security incidents at critical infrastructure facilities in Ukraine. Based on the analysis of the national regulatory framework, international standards (NIST SP 800-61 Rev. 3, ISO/IEC 27035:2023, ENISA CSIRT Maturity Framework) and cyber incident statistics for 2020–2025, a hybrid incident response lifecycle, a three-level CSIRT organizational model, and mandatory integration of the XDR+SOAR stack are proposed. 58 automated playbooks, a three-level personnel training system, and a simulation exercises programme (tabletop, red/purple team) have been developed. Pilot implementation at 19 critical infrastructure facilities demonstrated reduction of MTTD to 6.8 minutes, containment time to 11.4 minutes, MTTR (eradication) to 6.2 hours, recurrent incidents to 0.9 %, and ROI exceeding 10 000 % over three years. The scientific novelty lies in the comprehensive adaptation of advanced automation technologies to the specifics of Ukrainian legislation and hybrid threat conditions, which ensures surpassing international benchmarks in speed and economic efficiency.*

Keywords: *cybersecurity, incident response, critical infrastructure, lifecycle models, XDR, SOAR, CSIRT, playbook, automated response.*

Мирутенко Лариса Вікторівна, *к.т.н., доцент, доцент кафедри кібербезпеки та захисту інформації, Київський національний університет імені Тараса Шевченка.*
Myrutenko Larysa*, Ph.D., Associate Professor, Associate Professor of the Department of Cybersecurity and Information Protection, Taras Shevchenko National University of Kyiv.*

Пархоменко Іван Іванович*, к.т.н., доцент, завідувач кафедри кібербезпеки та захисту інформації, Київський національний університет імені Тараса Шевченка.*
Parkhomenko Ivan*, Ph.D., Associate Professor, Head of the Department of Cybersecurity and Information Protection, Taras Shevchenko National University of Kyiv.*

Мазур Іван Олександрович*, студент-магістр, кафедра кібербезпеки та захисту інформації, Київський національний університет імені Тараса Шевченка.*
Mazur Ivan*, Master's student, Department of Cybersecurity and Information Protection, Taras Shevchenko National University of Kyiv.*