https://doi.org/10.31891/2219-9365-2025-84-30
УДК 004.056

МЕЛЬНИК Мар'яна
Хмельницький національний університет
https://orcid.org/0009-0000-2137-8721
e-mail: melnyk.masia@gmail.com
ЧЕШУН Віктор
Хмельницький національний університет
https://orcid.org/0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua
ОЛЕКСЮК Дмитро
Хмельницький фаховий економіко-технологічний коледж УЕП
https://orcid.org/0009-0006-3735-1930
e-mail: oleksuk.dima@gmail.com
ЧЕШУН Дмитро
Хмельницький фаховий економіко-технологічний коледж УЕП
https://orcid.org/0009-0007-9937-9450
e-mail: dmitry_95@ukr.net

СИСТЕМОЛОГІЧНИЙ ПІДХІД ДО РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ В НОРМАТИВНО-ПРАВОВОМУ ПОЛІ УКРАЇНИ ТА МІЖНАРОДНИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Дослідження присвячене комплексному аналізу організаційних, методологічних та технологічних аспектів розслідування кіберінцидентів (DFIR) у державних інформаційних системах та на об'єктах критичної інфраструктури, що функціонують в умовах інтенсивних гібридних загроз. Обґрунтовано, що DFIR виконує стратегічну функцію, перетворюючись на механізм забезпечення національної кіберстійкості шляхом ітеративного застосування моделі NIST SP 800-61 Rev. 2 та вимог ISO/IEC 27035 щодо управління інцидентами та збереження доказів. Визначено критичні технологічні імперативи: впровадження SIEM та UEBA, а також обов'язкова інтеграція з платформами обміну MISP. Проведено компаративний аналіз міжнародних моделей і доведено оптимальність гібридного підходу для національної системи. Критичний огляд виявив системні дефіцити української практики: низький рівень автоматизації моніторингу, інституційну фрагментацію обміну індикаторами компрометації та гострий дефіцит фахівців із цифрової криміналістики. У зв'язку з цим, запропоновано комплексний, інтегрований метод розслідування, що передбачає уніфікацію процедур, імплементацію гібридної організаційної моделі та технологічне посилення через поєднання автоматизованих інструментів аналізу (SIEM, MISP) із формалізованими процедурами реагування. Реалізація підходу критична для скорочення часу розслідування та підвищення стійкості критичної інфраструктури.

Ключові слова: нормативно-правове регулювання, інформаційна безпека, цифрова криміналістика, розслідування кіберінцидентів.

MELNYK Mariana, CHESHUN Viktor
Khmelnytsky National University
OLEKSIUK Dmytro, CHESHUN Dmytro
Khmelnytskyi Vocational Economic and Technological College of the UEE

SYSTEMOLOGICAL APPROACH TO THE INVESTIGATION OF CYBER INCIDENTS IN THE REGULATORY AND LEGAL FIELD OF UKRAINE AND INTERNATIONAL INFORMATION SECURITY STANDARDS

This research provides a detailed and systemological analysis of the organizational, methodological, and technological dimensions of Digital Forensics and Incident Response (DFIR) implementation within governmental information systems and critical national infrastructure facilities. This operational domain is currently subjected to extreme pressure due to the intense and sustained nature of hybrid threats. The paper fundamentally substantiates that DFIR transcends a purely technical or reactive function, fulfilling a primary strategic role by transforming into a robust, cyclical mechanism essential for guaranteeing national cyber resilience and ensuring state stability. This crucial transformation is meticulously examined through the lens of recognized international standards, notably the four-phased model detailed in NIST SP 800-61 Rev. 2, and the stringent requirements of ISO/IEC 27035:2023 concerning incident management and the legally verifiable preservation of digital evidence. Key technical imperatives for achieving effective national response capabilities are clearly defined: these include the necessity for ubiquitous and consistent deployment of sophisticated Security Information and Event Management (SIEM) and User and Entity Behavior Analytics (UEBA) systems. Furthermore, the mandatory integration with specialized Threat Intelligence (TI) exchange platforms, such as the Malware Information Sharing Platform (MISP), is identified as a non-negotiable condition for achieving real-time threat synchronization and enabling coordinated containment actions. A critical review of existing national practices in Ukraine revealed pervasive systemic deficiencies. These structural weaknesses include a critically low level of monitoring automation, institutional fragmentation in the protocols for exchanging Indicators of Compromise (IoC), and a significant deficit of highly qualified digital forensics specialists. In direct response to these profound systemic shortcomings, a comprehensive, integrated cyber incident investigation methodology is formally proposed. Reinforcement is to be achieved through the symbiotic combination of automated analytical tools (including SIEM, MISP, and advanced forensic suites) with strictly formalized, standardized, and legally binding response and reporting procedures.

Keywords: regulatory and legal regulation, information security, digital forensics, cyber incident investigation.

Стаття надійшла до редакції / Received 03.11.2025
Прийнята до друку / Accepted 07.12.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Зі вступом світу в епоху тотальної цифровізації та прискореної трансформації державного сектору, де критично важливі послуги переносяться в онлайн-середовище, кількість, інтенсивність та складність кіберінцидентів постійно зростає, набуваючи загрозливих масштабів. Це явище стало глобальною тенденцією, що визначена як пріоритетний виклик для національної безпеки. Відповідно до ключових аналітичних звітів, зокрема, звіту Агенції Європейського Союзу з питань кібербезпеки ENISA [1], чітко простежується концентрація атак на життєво важливих секторах економіки та державного управління. За даними звіту, на ключові суб'єкти господарювання, які охоплюють державне управління, транспортну логістику, цифрову інфраструктуру та послуги, фінансовий сектор і промислове виробництво, припадає понад половина (53,7%) від загальної кількості зареєстрованих інцидентів. Це свідчить про те, що цілями зловмисників є саме ті системи, збій у роботі яких може спричинити найбільший соціальний та економічний ефект, що найчастіше робиться з метою шпигунства, економічного саботажу чи дестабілізації.

У відповідь на цю системну загрозу Європейський Союз ухвалив Директиву NIS2 про заходи для високого спільного рівня кібербезпеки в ЄС (EU Directive 2022/2555) [2], яка значно посилює вимоги до кіберстійкості організацій у ключових секторах, вводячи жорсткі зобов'язання щодо управління ризиками та звітності про інциденти. Цей нормативний акт відображає глобальне усвідомлення того, що кібербезпека більше не є лише технічною проблемою, а стратегічним питанням стійкості держави та суспільства.

В Україні, яка перебуває під постійним гібридним тиском, ця загрозлива тенденція підтверджується і набуває особливої гостроти. Звіти Державної служби спеціального зв'язку та захисту інформації (Держспецзв'язку) [3] та Команди реагування на комп'ютерні надзвичайні події України CERT-UA [4] фіксують не просто кількісне зростання, а й якісну еволюцію ворожих кібероперацій. Атаки стали більш цілеспрямованими, тривалими та складними, часто використовують комбінацію витончених тактик, технік і процедур (TTPs). До них належать масові кампанії соціальної інженерії та фішингу, націлені на персонал, атаки на ланцюги постачання програмного забезпечення та сервісів для компрометації кінцевих користувачів, а також застосування високодеструктивного шкідливого програмного забезпечення типу wiper – спеціалізованих програм, метою яких є не викрадення, а повне та незворотне знищення даних, що є характерним інструментом кібервійни [3]. Особливо зросла кількість цілеспрямованих атак, які концентруються на військових об'єктах та критичній інфраструктурі, що підтверджується активністю таких відомих російських угруповань, як UAC-0184 і UAC-0200 [4], які використовують кіберпростір як поле бою для збору розвідувальної інформації та порушення функціонування систем.

У такому екстремальному та постійно мінливому контексті розслідування кіберінцидентів (Digital Forensics and Incident Response – DFIR) стає не просто функцією, а критичним, незамінним елементом державної кібербезпеки. Його роль виходить далеко за межі звичайного усунення наслідків події та відновлення працездатності систем. Розслідування є єдиним надійним механізмом, що має забезпечувати накопичення якісних цифрових доказів із дотриманням ланцюга збереження (chain of custody), необхідних для встановлення юридичної відповідальності.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Систематизовані докази кіберзлочинів дозволяють провести глибокий аналіз першопричин інциденту (Root Cause Analysis), що включає ідентифікацію початкової точки проникнення (Initial Access), аналіз інструментів, що використовувалися зловмисником, та виявлення прихованих точок закріплення (Persistence) [5,6].

Отримані дані дозволяють сформувати детальний профіль загроз (Threat Profile), який є основою для стратегічного планування захисту [7]. Фахівці використовують результати розслідування для розуміння тактик, технік і процедур (TTPs), які використовують ворожі групи, та їхніх кінцевих цілей, що дозволяє проактивно розробляти та впроваджувати заходи запобігання подібним інцидентам у майбутньому [7,8].

В аналітичному звіті директора з корпоративного та брендового маркетингу кібербезпеки Xage Security [9] наведено огляд реальних інцидентів, що ілюструють еволюцію векторів атак на КІ. Серед них виявлення трьох нульових вразливостей у продуктах Cisco, відомих як ArcaneDoor, які були використані для компрометації ІТ-систем. Також наголошується на появі шкідливого ПЗ FrostyGoop, спеціально розробленого для експлуатації протоколу Modbus в середовищах ICS. Ці приклади прямо вказують на необхідність форензики, адаптованої до промислових протоколів, що вимагає специфічних знань та інструментів для розслідування.

Сучасні наукові дослідження в галузі цифрової криміналістики державного сектору та критичної інфраструктури (КІ) зосереджені на трьох ключових напрямках: автоматизація DFIR-процесів за допомогою штучного інтелекту, розробка моделей стійкості КІ до цільових атак та удосконалення методів управління інцидентами в умовах гібридних загроз.

Публікації останніх років, особливо українських та європейських авторів, містять потужний акцент на кіберстійкості та протидії державним (APT) атакам. У роботі [10] розроблено інноваційну, керовану даними модель кіберстійкості, призначену для оцінки та підвищення здатності КІ відновлюватися після кібератак. Автори підкреслюють, що у відповідь на складність загроз, захист і відновлення стають невідкладними потребами, а стійкість вимірюється не лише запобіганням, але й швидкістю та повнотою відновлення.

Дослідження [11] відзначає, що загрози КІ посилюються через складні атаки на ланцюги постачання, соціальну інженерію та використання нульових вразливостей. Вони виступають за посилення співпраці між державним і приватним секторами та впровадження архітектур Zero Trust для мінімізації ризику. Робота [12] конкретизує ці виклики, зазначаючи, що сучасні загрози вже не обмежуються вірусами чи фішингом, а включають державні APT-атаки, що використовують приховані та високоскладні методи для проникнення в мережі та саботажу, що робить розслідування набагато складнішим.

В роботі [13] авторами акцентовано увагу на необхідності комплексного аналізу ризиків. Автори формулюють модель загроз для КІ, виділяючи тріаду основних дій для захисту: впровадження ефективних заходів безпеки, регулярний моніторинг мереж та навчання персоналу.

У контексті КІ, де важлива не лише швидкість, але й точність, дослідження [14] пропонує гібридні алгоритми машинного навчання для проактивного пошуку загроз. Автори використовують реальні дані з відкритих джерел, що імітують аномалії в банківських транзакціях та SWIFT-атаках (типові для фінансової КІ), доводячи, що гібридні моделі ефективніші у виявленні аномалій у потоках даних у реальному часі.

Низка досліджень підкреслює необхідність автоматизації етапів цифрової криміналістики та реагування на інциденти (DFIR) через зростаючий обсяг даних та швидкість сучасних атак. У роботі [15] аналізується інтеграція машинного навчання та роботизованої автоматизації процесів (RPA) у DFIR-робочі процеси. Автори стверджують, що ручні DFIR-процеси є занадто ресурсомісткими та повільними для реагування на сучасні адаптивні загрози (наприклад, поліморфний зловмисний код). Застосування штучного інтелекту (ШІ) пропонується для автоматизації збору доказів, розпізнавання патернів атак та прискорення часових затримок, які виникають під час ручного аналізу журналів. Подібні висновки містяться і в дослідженні [16], де підкреслюється, що ШІ здатен трансформувати DFIR з реактивного процесу на проактивну, інтелектуальну систему безперервного захисту.

Особлива увага приділяється моделюванню загроз та управлінню інцидентами, зважаючи на унікальну складність операційних технологій (OT) та систем промислового контролю (ICS). У статті [17] пропонується метод управління IT-інцидентами в об'єктах критичної інформаційної інфраструктури (КІІ). Метод комбінує модель загроз STRIDE з методологією багатокритеріального прийняття рішень TODIM, що дозволяє систематично ідентифікувати, оцінювати та пріоритизувати загрози з урахуванням критичності об'єктів КІІ. Експериментальна валідація показала, що такий підхід суттєво покращує безпеку КІІ за рахунок систематичної пріоритизації ризиків.

Проаналізовані публікації демонструють загальносвітову тенденцію до переходу від реактивних до проактивних стратегій захисту. Наукова спільнота чітко зазначає, що виявлення та розслідування атак на державні органи та КІ вимагає парадигмального зсуву від традиційної IT-безпеки до адаптивних, автоматизованих та гібридних DFIR-систем, здатних працювати в умовах високої волатильності, складності та постійного геополітичного тиску.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є: формулювання концептуальних положень методу розслідування кіберінцидентів, орієнтованого для застосовування на об’єктах критичної інфраструктури України з урахуванням вимог чинного державного законодавства та міжнародних регулюючих документів.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Правові і організаційні аспекти виявлення та розслідування атак на об’єкти критичної інфраструктури

Створення та функціональна стійкість національних систем реагування на кіберінциденти та механізмів безперервного моніторингу є не просто технічною вимогою, а стратегічною умовою забезпечення національної кіберстійкості та функціональної цілісності державних інформаційних систем. Недотримання нормативно-правових та технічних вимог, які регламентуються законодавством України, створює системні вразливості, що ставлять під загрозу не лише дискретні організації, але й усю структуру державного управління.

У цих умовах розслідування кіберінцидентів відіграє ключову і, водночас, подвійну роль: тактичну та стратегічну. На тактичному рівні йдеться про оперативну ліквідацію наслідків атаки та відновлення функціональності. На стратегічному рівні DFIR є єдиним механізмом для збору достовірних цифрових доказів, встановлення кореневих причин події, визначення характерних ознак загроз та розробки адаптивних заходів запобігання схожим інцидентам у майбутньому.

Базове концептуальне визначення інциденту інформаційної безпеки надається міжнародним стандартом ISO/IEC 27035:2023 [18]. Цей документ визначає інцидент як подію або низку пов'язаних подій, які становлять реальну або потенційну загрозу для конфіденційності, цілісності чи доступності інформаційних ресурсів (C-I-A Triad). На практиці це охоплює будь-яку аномальну ситуацію, що вимагає негайної, регламентованої реакції з боку уповноважених суб'єктів.

Фундаментальною методологічною основою для організації процесу реагування є Керівництво щодо обробки інцидентів комп'ютерної безпеки Національного інституту стандартів і технологій США NIST SP 800-61 Rev. 2 [19]. Цей стандарт встановлює циклічну, чотирифазну модель, яка підкреслює ітеративний характер процесу розслідування:

– Фаза 1: підготовка (Preparation) – створення інституційної та технічної бази;
– Фаза 2: виявлення й аналіз (Detection and Analysis) – ідентифікація та верифікація інциденту;
– Фаза 3: реагування, стримування (ізоляція), ліквідація та відновлення (Containment, Eradication, and Recovery) – обмеження шкоди та повернення до нормальної роботи;
– Фаза 4: дії після завершення інциденту (Post-Incident Activity) – аналіз уроків та вдосконалення.

Такий підхід трансформує розслідування з реактивного інструменту на фундаментальний компонент кіберстійкості, забезпечуючи безперервне навчання системи та її адаптацію до динаміки кіберзагроз.

Перша фаза зосереджена на створенні формалізованої архітектури реагування. Формується команда реагування на інциденти (CSIRT), яка отримує чіткий мандат, прописуються політики безпеки, визначаються правила роботи з інцидентами (SOP) та створюються канали кризової комунікації – як внутрішні, так і зовнішні. З технічного погляду, критичною є побудова інфраструктури фіксації подій безпеки, що включає збір журналів системних подій, мережевого трафіку та аутентифікаційних подій [19,20]. Ця фаза також включає проактивну діяльність, таку як пошук прихованих загроз та створення високоточних образів систем (forensic images) для швидшого відновлення.

У фазі виявлення та аналізу для оперативного виявлення інцидентів застосовується централізована агрегація логів та подій. Зазвичай, для цього використовуються платформи Security Information and Event Management (SIEM), такі як Wazuh або ELK Stack. Ці системи забезпечують збір, нормалізацію, агрегацію та кореляцію величезних обсягів даних, перетворюючи розрізнені системні повідомлення на осмислені інциденти.

Ключовим завданням цього етапу є ідентифікація індикаторів компрометації. Це можуть бути незвичні спроби входу, підозрілі мережеві активності, маніпуляції з важливими файлами чи запуск аномальних процесів. Для підвищення ефективності виявлення застосовуються такі передові методики [20]:

– аналіз поведінки користувачів та сутностей (User and Entity Behavior Analytics, UEBA);
– системи виявлення вторгнень (IDS/IPS);
– машинне навчання (ML) та штучний інтелект (AI).

Аналіз поведінки користувачів та сутностей застосовується для иявлення аномалій, які відхиляються від встановлених базових ліній нормальної поведінки (наприклад, незвичний час доступу чи обсяг завантажених даних). Системи виявлення вторгнень здійснюють моніторинг мережевого трафіку на основі сигнатур або аномалій. Машинне навчання та ШІ використовуються для автоматичної класифікації подій, виявлення Zero-Day атак та зменшення кількості хибних спрацьовувань тощо.

Етап реагування, стримування, ліквідації та відновлення є найбільш критичним у часовому вимірі. Його головна мета – припинити поширення атаки, зменшити її наслідки та повернути систему до нормального режиму роботи. Стримування включає ізоляцію пошкоджених систем шляхом їх відключення від мережі або застосування мікросегментації для обмеження латерального руху зловмисника. Ліквідація вимагає глибокого форензичного аналізу для видалення всіх прихованих бекдорів, шкідливих файлів та модифікацій, внесених зловмисником. Відновлення базується на перевірці та розгортанні криптографічно чистих резервних копій та встановленні оновлень.

У міжнародному досвіді цей процес посилюється інтеграцією з платформами обміну інформацією про загрози, такими як MISP (Malware Information Sharing Platform) [21]. Це дозволяє командам оперативно обмінюватися індикаторами компрометації (IoC), що значно підвищує швидкість і точність ідентифікації природи загрози. У державних структурах України цей процес обов'язково регламентується затвердженими політиками реагування та узгоджується з органами Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ) [3,21].

На фінальному етапі (фаза діяльності після інциденту) проводиться детальний аналіз першопричин (RCA) для виявлення фундаментальних прогалин, які дозволили інциденту статися. Результатом є формування технічного звіту, оцінка ефективності застосованих заходів реагування та розробка обґрунтованих рекомендацій для уникнення подібних випадків. Ключовим елементом цієї фази є забезпечення юридичної значущості зібраних артефактів. Стандарт ISO/IEC 27035-3:2020 [22] та вимоги цифрової криміналістики наголошують на необхідності бездоганного документування доказів із дотриманням ланцюга збереження (Chain of Custody), включаючи створення форензичних образів носіїв інформації та підтвердження їхньої цілісності за допомогою криптографічного хешування. Це необхідно для подальшого

використання матеріалів у судових або адміністративних розслідуваннях.

Організаційна структура національного реагування на кіберінциденти суттєво варіюється. Сформувалися три основні моделі:

- централізована модель (Європейський Союз);
- децентралізована модель (Сполучені Штати Америки);
- гібридна/змішана модель (країни Балтії).

В централізованій моделі головну роль виконує єдиний національний або наднаціональний центр реагування (CERT/CSIRT), який відповідає за координацію, стандартизацію та обмін інформацією з усіма галузевими та відомчими командами. Прикладом є CERT-EU [21], який забезпечує взаємодію та реагування на кіберінциденти в інституціях Європейського Союзу, підтримуючи єдиний, узгоджений рівень безпеки відповідно до вимог директиви NIS2. Перевага централізованій моделі у високій упорядкованості дій, централізованому зборі національного профілю загроз та ефективній координації при великомасштабних інцидентах.

В децентралізованій моделі США кожна відомча структура або сектор КІ має власну, значною мірою автономну команду реагування. Зокрема, Міністерство енергетики (DOE), Департамент внутрішньої безпеки (DHS) та Агентство з кібербезпеки і безпеки інфраструктури (CISA) мають окремі, але взаємодіючі підрозділи. Координація відбувається через федеральні протоколи та платформи обміну інформацією (ISACs). Перевага децентралізованої моделі – швидкість реагування у межах власної юрисдикції, глибока доменна експертиза у специфічних секторах (наприклад, енергетика чи фінанси).

Гібридна модель поєднує елементи обох моделей: національний центр кібербезпеки встановлює єдині методологічні стандарти та політики, тоді як безпосереднє реагування здійснюють відомчі підрозділи. Прикладом є Литва та Естонія [23]. Естонія, зокрема, створила добровольче формування Cyber Defence League, яке інтегрує державних і громадських фахівців для участі у розслідуванні масштабних кіберінцидентів, як це було під час масових атак у 2007 році. Ця система забезпечує гнучкість у реагуванні та мобілізацію ресурсів, зберігаючи при цьому централізований контроль над аналітикою.

В Україні процес розслідування кіберінцидентів на об’єктах КІ регламентується Законами «Про основні засади забезпечення кібербезпеки України» [24], «Про захист інформації в інформаційно-телекомунікаційних системах» [25] та Постановою Кабінету Міністрів №518 від 19 червня 2019 року [26], що деталізує порядок реагування. Однак, попри наявність нормативної бази та методичних рекомендацій CERT-UA [21,27], система розслідування стикається з низкою системних проблем, що обмежують її ефективність, особливо в умовах інтенсивних гібридних атак.

Одним із найбільш критичних недоліків є низький рівень автоматизації процесів збору та аналізу подій безпеки. За даними Держспецзв’язку, лише близько 40% об’єктів КІ мають впроваджені системи моніторингу безпеки SIEM [3]. Це означає, що у більшості державних установ моніторинг здійснюється фрагментарно, без централізованої кореляції логів, що ускладнює оперативне виявлення та формування цілісної картини інциденту. На відміну від країн ЄС, де системи Wazuh або ELK Stack інтегруються з платформами обміну MISP [21], в Україні інфраструктура моніторингу залишається горизонтально фрагментованою. Кожен об’єкт часто використовує власні засоби виявлення аномалій, що призводить до різного рівня деталізації даних та істотно ускладнює централізований аналіз загроз.

Недостатня інтеграція між національною CERT-UA та галузевими/відомчими CSIRT-командами призводить до затримки обміну критичною інформацією про атаки та неузгодженості дій під час реагування. Рекомендації ENISA [28] вимагають, щоб ефективна модель взаємодії ґрунтувалася на принципі взаємного обміну даними в режимі реального часу, проте в Україні цей обмін ще не є системним та стандартизованим. Відсутність уніфікованої національної бази індикаторів компрометації, інтегрованої через формати STIX/TAXII [29], як це реалізовано в європейських країнах, змушує команди реагування працювати з застарілими або неповними даними, що значно знижує швидкість виявлення повторюваних атак.

Суттєвою проблемою залишається нестача висококваліфікованих фахівців із цифрової криміналістики (Digital Forensics). Це обмежує спроможність оперативно проводити глибокий технічний аналіз інцидентів (форензика кінцевих точок, мережева форензика, аналіз шкідливого коду). Процес розслідування затримується через дефіцит спеціалістів, здатних професійно застосовувати інструменти, такі як Autopsy, FTK Imager, Volatility (для аналізу дампу пам'яті) чи Wireshark (для мережевого аналізу), з дотриманням криміналістичних вимог. Наявність технічних артефактів без належної експертизи для їхнього аналізу та інтерпретації є недостатньою для встановлення механізмів компрометації та цілей зловмисника.

Крім того, відсутність єдиного формату звітності про інциденти, незважаючи на існування ISO/IEC 27035 [18,22] та методичних рекомендацій CERT-UA [27], створює додаткові труднощі для обміну інформацією між відомствами та для подальшого використання матеріалів у судових процесах. Належне документування та звітність є невід’ємною частиною post-incident activity і має забезпечувати відтворюваність та прозорість розслідування.

Комплексний підхід до виявлення та розслідування кіберінцидентів

Для подолання виявлених системних проблем, які критично обмежують ефективність національної кібербезпеки в умовах перманентних гібридних атак, необхідна розробка та впровадження комплексного підходу до виявлення та розслідування інцидентів. Цей підхід має ґрунтуватися на глибокій інтеграції технологічних рішень та організаційно-процедурної уніфікації. На технологічному рівні метод повинен забезпечити автоматизований, безперервний збір та інтелектуальний аналіз подій безпеки. Це досягається за рахунок щільної інтеграції платформ SIEM/ELK (для агрегації та кореляції логів) з системами SOAR (Security Orchestration, Automation and Response), які автоматизують рутинні операції реагування, скорочуючи час, необхідний для первинного стримування. На процедурному рівні критично важливим є запровадження формалізованих і стандартизованих процедур реагування (на основі NIST SP 800-61 Rev. 2 та ISO/IEC 27035), що гарантує юридичну достовірність зібраних доказів та повноту охоплення всіх етапів інциденту. Крім того, ключовим елементом інтеграції є забезпечення системного обміну інформацією про загрози (Threat Intelligence) на національному рівні через стандартизовані платформи (як-от MISP та формати STIX/TAXII), що дозволяє швидко виявляти повторювані або схожі атаки на різних об’єктах критичної інфраструктури.

Реалізація такого інтегрованого підходу дозволить кардинально підвищити оперативну ефективність реагування на інциденти, скоротити середній час розслідування (Dwell Time – час перебування зловмисника в мережі) та мінімізувати ризики повторного компрометування об’єктів КІ. Це, у свою чергу, є критично важливим для забезпечення сталої кіберстійкості держави в цілому.

Запропонований спосіб розслідування кіберінцидентів базується на фундаментальних принципах циклічності, комплексності та стандартизації. Його стратегічною метою є створення універсального, верифікованого алгоритму дій, який охоплює повний життєвий цикл інциденту – від проактивного виявлення ознак аномалії до формування детальних висновків та обґрунтованих рекомендацій щодо удосконалення архітектури безпеки інформаційних систем. На відміну від традиційних, лінійних підходів, орієнтованих переважно на ізольований аналіз технічних артефактів (форензику), запропонована модель передбачає нерозривну інтеграцію організаційних, процедурних і технічних компонентів у єдину, керовану систему реагування. Ця інтеграція дозволяє значно скоротити середній час реагування на інцидент, підвищити точність класифікації загроз завдяки постійному обміну TI та забезпечити бездоганну узгодженість дій між усіма суб’єктами кібербезпеки (CERT-UA, відомчі CSIRT та експертні групи).

Метод передбачає, що розслідування кіберінцидентів здійснюється як жорстка послідовність п'яти взаємозалежних етапів, де кожен має чітко визначену мету, контрольовані вхідні та вихідні дані, стандартизований набір застосованих інструментів і чітко призначених відповідальних осіб. Для забезпечення цієї послідовності та взаємодії критично важливу роль відіграють платформи Wazuh (для збору та моніторингу EDR), ELK Stack (для централізованої аналітики), MISP (для обміну TI) та TheHive (як платформа керування інцидентами, що координує всі дії). Всі ці компоненти інтегруються у єдине, високонадійне інформаційне середовище реагування, що мінімізує людський фактор та підвищує прозорість процесу.

Деталізація етапів приведена в таблиці 1.

Таблиця 1

Етапи методу розслідування кіберінцидентів

Етап	Основна мета	Ключові дії	Очікувані результати
Ідентифікація	Виявлення інциденту	Збір логів, аналіз SIEM, фіксація події	Первинне повідомлення
Класифікація	Визначення типу і пріоритету	Порівняння з базами IOC, оцінка ризику	Присвоєння рівня критичності
Технічний аналіз	Встановлення джерела та механізму	Форензичний аналіз, перевірка логів, реверс шкідливого ПЗ	Виявлення причин інциденту
Відновлення	Усунення наслідків	Відновлення даних, оновлення конфігурацій	Відновлена система
Документування	Збереження знань	Підготовка звіту, внесення в бази MISP	База знань для попередження атак

На етапі ідентифікації інциденту проводиться систематичний і безперервний збір інформації про потенційні події безпеки. Джерелами цієї інформації виступають різноманітні телеметричні та логістичні дані, зокрема: системні журнали операційних систем та додатків, мережеві потоки (NetFlow), сигнали від систем виявлення та запобігання вторгнень (IDS/IPS), агреговані дані з платформ SIEM, а також повідомлення, отримані від кінцевих користувачів або внутрішніх підрозділів. Основна мета цього етапу полягає у виявленні будь-яких аномалій, що критично виходять за межі типової чи заздалегідь встановленої базової поведінки мережі, інфраструктури або окремих облікових записів користувачів.

Після первинної фіксації події та її валідації аналітичною системою, ключовим завданням стає визначення, чи є вона дійсним кіберінцидентом (уникаючи хибних спрацьовувань) та встановлення її критичності згідно з внутрішніми політиками та міжнародними стандартами. Аналітик відділу реагування здійснює оперативне порівняння виявлених індикаторів компрометації, таких як підозрілі IP-адреси, шкідливі

домени, криптографічні хеші потенційно скомпрометованих файлів або аномальні патерни взаємодії, із записами у базі MISP. Цей крос-аналіз із зовнішніми та внутрішніми базами загроз дозволяє швидко підтвердити природу та походження атаки, що є критично важливим для переходу до наступних, більш рішучих дій зі стримування та ліквідації. Процес вимагає високої точності та швидкості для мінімізації часу перебування зловмисника в системі.

Додатково проводиться оцінка потенційного впливу за критеріями:

- масштаб порушення (локальний, корпоративний, національний);
- категорія активу, на який здійснено вплив (система керування, сервер, користувацька станція);
- наявність загрози безперервності бізнес-процесів.

На цьому етапі класифікації події формується обґрунтоване рішення щодо подальшої долі інциденту: чи передати його для повноцінного розслідування, залучивши форензичні ресурси, чи обмежитися посиленим моніторингом, якщо ризики визнані низькими. Результатом класифікації є присвоєння інциденту рівня пріоритетності реагування, який безпосередньо визначає склад команди, обсяг фінансових та технічних ресурсів, що будуть задіяні у подальшому процесі, а також встановлює граничні терміни для стримування та ліквідації.

Технічний етап розслідування, який часто називають саме цифровою криміналістикою, є найбільш складним, критичним і ресурсомістким. Він охоплює методологічний збір та обробку цифрових артефактів з усіх скомпрометованих або потенційно скомпрометованих вузлів, а також глибокий форензичний аналіз цих даних. Цей процес є єдиним способом забезпечити встановлення точного механізму атаки, ідентифікувати джерело компрометації (точку входу) та оцінити повні потенційні наслідки вторгнення. Ключова особливість криміналістичного етапу полягає у суворій вимозі: під час аналізу цифрових доказів не допускається їхня модифікація. Тому вся робота проводиться виключно з криптографічно перевіреними копіями (форензичними образами) оригінальних носіїв, що гарантує дотримання ланцюга збереження доказів. Після завершення аналізу збирається детальний ланцюжок подій, який відображає послідовну хронологію дій зловмисника, що дозволяє побудувати вичерпну причинно-наслідкову модель інциденту.

Етап відновлення передбачає комплексне усунення наслідків атаки та повернення скомпрометованих систем до їхнього доінцедентного, стабільного стану. Проводиться відновлення функціональності та даних з чистих, перевірених резервних копій, перевірка цілісності критичних баз даних та конфігураційних файлів, обов'язкове оновлення та скидання облікових записів користувачів з підвищеними привілеями, а також, що є найважливішим, усунення першопричинних вразливостей, через які було здійснено вторгнення. Особливу увагу приділяють системам моніторингу та захисту, які вдосконалюються з урахуванням виявлених уразливостей. Відновлення завершується фінальною верифікацією цілісності цифрових підписів, аутентифікаційних логів та сертифікатів безпеки, що підтверджує успішну ліквідацію.

Після остаточного усунення інциденту всі виконані дії, отримані докази та прийняті рішення повинні бути ретельно задокументовані для формування звіту та аналізу уроків. Формується звіт про розслідування (Incident Report), який містить:

- хронологію подій;
- опис знайдених артефактів;
- результати технічного аналізу;
- рекомендації щодо запобігання подібним подіям.

Дані про інцидент публікуються у MISP, що сприяє обміну інформацією між національними та галузевими CSIRT-командами. Зібрані індикатори надалі використовуються для вдосконалення систем виявлення атак, а також для тренування персоналу на реальних кейсах.

Запропонований метод орієнтований на взаємодію автоматизованих систем і людського фактору. На архітектурному рівні він передбачає взаємодію таких компонентів:

- wazuh/elk stack, виявлення інцидентів, первинна обробка подій;
- thehive – управління кейсами, розподіл завдань між аналітиками;
- misp, обмін індикаторами компрометації, інтеграція з зовнішніми базами даних;
- forensic tools (autopsy, volatility, ftk imager), технічне підтвердження інциденту.

Таким чином, формується замкнутий цикл реагування, де кожен інцидент стає джерелом знань для вдосконалення політик безпеки.

Перевагами пропонованого методу є масштабованість, а саме те, що метод може застосовуватись як у державних органах, так і в комерційних структурах. Сумісність із міжнародними стандартами дозволяє інтегрувати його у національну систему кіберзахисту. Використання Wazuh та TheHive дозволяє зменшити вплив людського фактору та автоматизацію процесів. Кожне розслідування поповнює базу знань, яка використовується для навчання аналітиків [26]. Усі звіти мають єдину структуру, що спрощує взаємодію між командами реагування.

Запропонований метод розслідування кіберінцидентів є комплексною системою, яка забезпечує не лише технічне реагування на події безпеки, а й стратегічне управління кіберризиками. Його впровадження дозволяє створити єдиний стандарт дій для суб’єктів, що обслуговують об’єкти критичної інформаційної інфраструктури.

Метод забезпечує повну трасованість дій, прозорість збору доказів та підвищення ефективності реагування. Завдяки інтеграції інструментів відкритого коду, таких як Wazuh, MISP, TheHive та ELK Stack, він не потребує значних фінансових витрат і може бути реалізований у державних або корпоративних системах моніторингу безпеки.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

За результатами проведеного дослідження було досягнуто глибокого розуміння системних та операційних аспектів розслідування кіберінцидентів у державному секторі та на об'єктах критичної інфраструктури, особливо в умовах інтенсивних гібридних загроз. Доведено, що розслідування кіберінцидентів виконує стратегічну, а не лише тактичну функцію, трансформуючись із засобу ліквідації наслідків на фундамент національної кіберстійкості. Дослідження формалізувало цей процес на основі міжнародних стандартів, зокрема циклічної чотирифазної моделі NIST SP 800-61 Rev. 2 та визначень ISO/IEC 27035.

Критичний огляд національної системи розслідування виявив системні недоліки, які обмежують її ефективність. Зокрема, було встановлено низький рівень автоматизації процесів моніторингу, фрагментацію інфраструктури та недостатню інтеграцію між секторальними та національними командами реагування.

Для підвищення ефективності процесу розслідування кіберінцидентів запропоновано системологічний підхід, реалізований в нормативно-правовому полі України та міжнародних стандартів інформаційної безпеки.

Запропонований підхід до розслідування кіберінцидентів базується на ідеї комплексного збору, кореляції та аналізу подій безпеки з різних рівнів інформаційної системи. Його основою є поєднання централізованого моніторингу, цифрової криміналістики та обміну інформацією про загрози, що дозволяє розглядати інцидент не як окрему подію, а як послідовний процес із чіткою логікою розвитку.

Метод орієнтований на використання агентного моніторингу кінцевих вузлів, централізованого збору журналів та аналітичних платформ, які забезпечують збереження цілісності цифрових доказів і можливість відтворення хронології подій. Особливу увагу приділено тому, щоб кожен етап розслідування, від виявлення підозрілої активності до відновлення системи, був формалізований і міг бути повторений незалежно від типу інциденту. Концепція методу передбачає інтеграцію різних джерел даних: системних журналів операційних систем, подій безпеки, мережевої активності та артефактів файлової системи. Це дозволяє компенсувати втрату або спотворення окремих даних за рахунок багатоканального збору інформації та підвищує стійкість методу до спроб приховування слідів атаки.

Література

1. ENISA Threat Landscape 2025. European Union Agency for Cybersecurity (ENISA). 2025. URL: https://h7.cl/1l8EO
2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). European Union. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
3. Річний звіт 2024: системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: http://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006
4. Огляд кіберзагроз та стратегій захисту в 2025 році: досвід CERT-UA. URL: https://h7.cl/1l8ED
5. Evolution Cybercrime – Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data / Muhammad Abdullah, Muhammad Munib Nawaz, Bilal Saleem, Maila Zahra, Effa binte Ashfaq, Zia Muhammad. Analytics. 2025. № 4(3):25. https://doi.org/10.3390/analytics4030025
6. Duraid Thamer Salim, Manmeet Mahinderjit Singh, Pantea Keikhosrokiani. A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model. Heliyon. 2023. Volume 9, Issue 7. https://doi.org/10.1016/j.heliyon.2023.e17156
7. Evolving techniques in cyber threat hunting: A systematic review / Arash Mahboubi et al. Journal of Network and Computer Applications. 2024. Volume 232. https://doi.org/10.1016/j.jnca.2024.104004
8. Gulbay Burak, Demirci Mehmet. A Framework for Developing Strategic Cyber Threat Intelligence from Advanced Persistent Threat Analysis Reports Using Graph-Based Algorithms. Preprints.org. 2024. https://orcid.org/10.20944/preprints202407.1408.v1
9. Celine Rosak. 2024 in Review: Cyber Threats and the Fight to Secure Critical Infrastructure. Global Security Magazine. 2024. URL: https://h7.cl/1gfjs
10. Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience / Muharman Lubis, Muhammad Fakhrul Safitra, Hanif Fakhrurroja, Alif Noorachmad Muttaqin. Sensors. 2025. № 25(15):4545. https://doi.org/10.3390/s25154545

11. Protecting the cybersecurity of critical infrastructures and their supply chains. ICC Working Paper. 2024. 35 p. URL: https://h7.cl/1l8E5
12. Rajender Pell Reddy. Cybersecurity for Critical Infrastructure: Protecting National Assets in the Digital Age. International Journal of Computer Trends and Technology (IJCTT). 2025. Vol. 73, № 2. P. 7-17. https://doi.org/10.14445/22312803/IJCTT-V73I2P102
13. Cybersecurity challenges and solutions for critical infrastructure protection / A. Tkachov, R. Korolov, I. Rahimova, I. Aksonova. Ukrainian Scientific Journal of Information Security. 2024. Vol. 30, issue 1. P. 58-66. https://doi.org/10.18372/2225-5036.30.18604
14. Shan A., Myeong S. Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. Sensors. 2024. № 24(15):4888. https://doi.org/10.3390/s24154888
15. John Kuforiji. Digital Forensics and Incident Response (DFIR) Automation: Leveraging AI to Accelerate Breach Investigation, Evidence Collection, and Cyberattack Mitigation. Journal of Data Analysis and Critical Management. 2025. Vol. 1, № 04. https://doi.org/10.64235/tsvfvz27
16. Artificial intelligence integration in cyber incident response teams to enable faster containment, forensic accuracy, and resilient business continuity / Kwaku Gyamfi Boamah, AFUA Asante, Ashley Timean, Kwadwo Fening Okai. International Journal of Science and Research Archive. 2025. №17(01). P.1263-1280. https://doi.org/10.30574/ijsra.2025.17.1.2933
17. Method for managing IT incidents in critical information infrastructure facilities / S. Gnatyuk, V. Sydorenko, A. Polozhentsev, V. Sokolov. CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II. 2024. URL: https://h7.cl/1l8Dk
18. ISO/IEC 27035-1:2023 Information technology – Information security incident management – Part 1: Principles and process. International Organization for Standardization. 2023. URL: https://h7.cl/1gdGl
19. NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide. URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final
20. NIST SP 800-61r3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management – A CSF 2.0 Community Profile / Alex Nelson et al. National Institute of Standards and Technology. URL: https://h7.cl/1l6Xp
21. Роз'яснення CERT-UA: платформа MISP, що це, як підключатися та які переваги. Державна служба спеціального зв'язку та захисту інформації України. URL: https://h7.cl/1gfiS
22. ISO/IEC 27035-3:2020 Information technology – Information security incident management – Part 3: Guidelines for ICT incident response operations. International Organization for Standardization, 2020. URL: https://www.iso.org/ru/standard/74033.html
23. Górka Marek. Baltic States Cyber Security Policy: Development of digital capabilities in 2017–2022. Stosunki Międzynarodowe – International Relations. Vol. 59. 2023. P. 57-81. https://doi.org/10.12688/stomiedintrelat.17684.1
24. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : редакція від 19.10.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
25. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : редакція від 20.04.2025. URL: https://h7.cl/1l8Dv
26. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019 № 518 : редакція від 20.11.2025. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
27. Наказ Адміністрації Держспецзв'язку від 03.12.2025 №798 «Про затвердження Методичних рекомендацій щодо типових вимог до підрозділів з кіберзахисту, загальних вимог до керівників з кіберзахисту в органах державної влади, а також до відповідальних осіб, які виконують функції та завдання керівника з кіберзахисту в юридичних особах, що є власниками або розпорядниками об'єктів критичної інформаційної інфраструктури I і II категорій критичності, та в органах місцевого самоврядування». Державна служба спеціального зв'язку та захисту інформації України. URL: https://h7.cl/1l6XU (дата звернення: 3.12.2025).
28. Best practices for cyber crisis management. European Union Agency for Cybersecurity (ENISA). 2024. URL: https://h7.cl/1l6lr
29. Cybersecurity Incident & Vulnerability Response Playbooks. Cybersecurity and Infrastructure Security Agency (CISA). 2021. 44 p. URL: https://h7.cl/1gd8H

References

1. ENISA Threat Landscape 2025. European Union Agency for Cybersecurity (ENISA). 2025. URL: https://h7.cl/1l8EO
2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). European Union. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
3. Richnyy zvit 2024: systemy vyyavlennya vrazlyvostey i reahuvannya na kiberintsydenty ta kiberataky. Operatyvnyy tsentr reahuvannya na kiberintsydenty Derzhavnoho tsentru kiberzakhystu Derzhavnoyi sluzhby spetsialnoho zvyazku ta zakhystu informatsiyi Ukrayiny. URL: http://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006
4. Ohlyad kiberzahroz ta stratehiy zakhystu v 2025 rotsi: dosvid CERT-UA. URL: https://h7.cl/1l8ED

5. Evolution Cybercrime – Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data / Muhammad Abdullah, Muhammad Munib Nawaz, Bilal Saleem, Maila Zahra, Effa binte Ashfaq, Zia Muhammad. Analytics. 2025. № 4(3):25. https://doi.org/10.3390/analytics4030025

6. Duraid Thamer Salim, Manmeet Mahinderjit Singh, Pantea Keikhosrokiani. A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model. Heliyon. 2023. Volume 9, Issue 7. https://doi.org/10.1016/j.heliyon.2023.e17156

7. Evolving techniques in cyber threat hunting: A systematic review / Arash Mahboubi et al. Journal of Network and Computer Applications. 2024. Volume 232. https://doi.org/10.1016/j.jnca.2024.104004

8. Gulbay Burak, Demirci Mehmet. A Framework for Developing Strategic Cyber Threat Intelligence from Advanced Persistent Threat Analysis Reports Using Graph-Based Algorithms. Preprints.org. 2024. https://orcid.org/10.20944/preprints202407.1408.v1

9. Celine Rosak. 2024 in Review: Cyber Threats and the Fight to Secure Critical Infrastructure. Global Security Magazine. 2024. URL: https://h7.cl/1gfjs

10. Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience / Muharman Lubis, Muhammad Fakhrul Safitra, Hanif Fakhrurroja, Alif Noorachmad Muttaqin. Sensors. 2025. № 25(15):4545. https://doi.org/10.3390/s25154545

11. Protecting the cybersecurity of critical infrastructures and their supply chains. ICC Working Paper. 2024. 35 p. URL: https://h7.cl/1l8E5

12. Rajender Pell Reddy. Cybersecurity for Critical Infrastructure: Protecting National Assets in the Digital Age. International Journal of Computer Trends and Technology (IJCTT). 2025. Vol. 73, № 2. P. 7-17. https://doi.org/10.14445/22312803/IJCTT-V73I2P102

13. Cybersecurity challenges and solutions for critical infrastructure protection / A. Tkachov, R. Korolov, I. Rahimova, I. Aksonova. Ukrainian Scientific Journal of Information Security. 2024. Vol. 30, issue 1. P. 58-66. https://doi.org/10.18372/2225-5036.30.18604

14. Shan A., Myeong S. Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. Sensors. 2024. № 24(15):4888. https://doi.org/10.3390/s24154888

15. John Kuforiji. Digital Forensics and Incident Response (DFIR) Automation: Leveraging AI to Accelerate Breach Investigation, Evidence Collection, and Cyberattack Mitigation. Journal of Data Analysis and Critical Management. 2025. Vol. 1, № 04. https://doi.org/10.64235/tsvfvz27

16. Artificial intelligence integration in cyber incident response teams to enable faster containment, forensic accuracy, and resilient business continuity / Kwaku Gyamfi Boamah, AFUA Asante, Ashley Timean, Kwadwo Fening Okai. International Journal of Science and Research Archive. 2025. №17(01). P.1263-1280. https://doi.org/10.30574/ijsra.2025.17.1.2933

17. Method for managing IT incidents in critical information infrastructure facilities / S. Gnatyuk, V. Sydorenko, A. Polozhentsev, V. Sokolov. CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II. 2024. URL: https://h7.cl/1l8Dk

18. ISO/IEC 27035-1:2023 Information technology – Information security incident management – Part 1: Principles and process. International Organization for Standardization. 2023. URL: https://h7.cl/1gdGl

19. NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide. URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final

20. NIST SP 800-61r3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management – A CSF 2.0 Community Profile / Alex Nelson et al. National Institute of Standards and Technology. URL: https://h7.cl/1l6Xp

21. Rozyasnennya CERT-UA: platforma MISP, shcho tse, yak pidklyuchatysya ta yaki perevahy. Derzhavna sluzhba spetsialnoho zvyazku ta zakhystu informatsiyi Ukrayiny. URL: https://h7.cl/1gfiS

22. ISO/IEC 27035-3:2020 Information technology – Information security incident management – Part 3: Guidelines for ICT incident response operations. International Organization for Standardization, 2020. URL: https://www.iso.org/ru/standard/74033.html

23. Górka Marek. Baltic States Cyber Security Policy: Development of digital capabilities in 2017–2022. Stosunki Międzynarodowe – International Relations. Vol. 59. 2023. P. 57-81. https://doi.org/10.12688/stomiedintrelat.17684.1

24. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny : Zakon Ukrayiny vid 05.10.2017 № 2163-VIII : redaktsiya vid 19.10.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

25. Pro zakhyst informatsiyi v informatsiyno-komunikatsiynykh systemakh : Zakon Ukrayiny vid 05.07.1994 № 80/94-VR : redaktsiya vid 20.04.2025. URL: https://h7.cl/1l8Dv

26. Pro zatverdzhennya Zahalnykh vymoh z kiberzakhystu obyektiv krytychnoyi infrastruktury : Postanova Kabinetu Ministriv Ukrayiny; Vymohy, Perelik vid 19.06.2019 № 518 : redaktsiya vid 20.11.2025. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

27. Nakaz Administratsiyi Derzhspetszvyazku vid 03.12.2025 №798 «Pro zatverdzhennya Metodychnykh rekomendatsiy shchodo typovykh vymoh do pidrozdiliv z kiberzakhystu, zahalnykh vymoh do kerivnykiv z kiberzakhystu v orhanakh derzhavnoyi vlady, a takozh do vidpovidalnykh osib, yaki vykonuyut funktsiyi ta zavdannya kerivnyka z kiberzakhystu v yurydychnykh osobakh, shcho ye vlasnykamy abo rozporyadnykamy obyektiv krytychnoyi informatsiynoyi infrastruktury I i II katehoriy krytychnosti, ta v orhanakh mistsevoho samovryaduvannya». Derzhavna sluzhba spetsialnoho zvyazku ta zakhystu informatsiyi Ukrayiny. URL: https://h7.cl/1l6XU

28. Best practices for cyber crisis management. European Union Agency for Cybersecurity (ENISA). 2024. URL: https://h7.cl/1l6lr

29. Cybersecurity Incident & Vulnerability Response Playbooks. Cybersecurity and Infrastructure Security Agency (CISA). 2021. 44 p. URL: https://h7.cl/1gd8H