МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Віктор ГНАТЮК
“_____”_____2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Методи та моделі управління кіберінцидентами у кризових ситуаціях в організаціях та підприємствах критичної інфраструктури»

Виконавець: _____ Олександр МАТВІЙЧУК-ЮДІН
(підпис)
Керівник: _____ Георгій КОНАХОВИЧ
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант з розділу «Охорона праці» _____ Катерина КАЖАН
(підпис)
Консультант з розділу «Охорона навколишнього середовища»
_____ Лариса ЧЕРНЯК
(підпис)
Нормконтролер: _____ Богдан ЧУМАЧЕНКО
(підпис)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Електронні комунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Віктор ГНАТЮК
“_____”_____2025 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

Матвійчука-Юдіна Олександра Олександровича

(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Методи та моделі управління кіберінцидентами у кризових ситуаціях в організаціях та підприємствах критичної інфраструктури» затверджена наказом ректора від «28» вересня 2025 р. №1965/ст
2. Термін виконання роботи: з 02.10.2025 р. по 31.12.2025 р.
3. Вихідні дані до роботи: CYBER INCIDENT MANAGEMENT, CRITICAL INFRASTRUCTURE, SOC, CSIRT, INCIDENT RESPONSE LIFE CYCLE, NIST SP 800-61, ISO/IEC 27035, ISO/IEC 27005, RISK ASSESSMENT MODELS, THREAT INTELLIGENCE, VULNERABILITY SCANNING, IDS, IPS, SIEM, SOAR, EDR/NDR, SCADA/ICS SECURITY, MITRE ATT&CK, CYBER KILL CHAIN, OODA LOOP, PDCA MODEL, AUTOMATION, CRISIS MANAGEMENT, RESILIENCE, RISK MITIGATION, RESOURCE OPTIMIZATION, CYBER THREAT ANALYSIS, INCIDENT PRIORITIZATION, RESPONSE METRICS.
4. Зміст пояснювальної записки: Аналіз сучасного стану управління кіберінцидентами та нормативно-правові основи діяльності критичної

інфраструктури; класифікація та ідентифікація загроз і вразливостей у критичній інфраструктурі; існуючі методи та моделі реагування на кіберінциденти у кризових умовах; методика та модель управління кіберінцидентами в кризових ситуаціях.

5. Перелік обов'язкового графічного (ілюстрованого) матеріалу: Схема моделі життєвого циклу інциденту, класифікаційна таблиця загроз за галузевими доменами критичної інфраструктури, діаграма типового ланцюга атаки, модель архітектури SOC/CSIRT у системі управління кіберінцидентами, схема інтеграції інструментів моніторингу у єдину систему управління, комунікаційна схема координації дій між державними структурами та операторами критичної інфраструктури, модель взаємодії підрозділів безпеки, модель плану реагування на кіберінциденти.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст кваліфікаційної роботи	02.10.2025-04.10.2025	Виконано
2	Вступ	05.10.2025-08.10.2025	Виконано
3	Аналіз сучасного стану управління кіберінцидентами	09.10.2025-22.10.2025	Виконано
4	Класифікація загроз і вразливостей	23.10.2025-05.11.2025	Виконано
5	Розробка моделі управління кіберінцидентами	06.11.2025-30.11.2025	Виконано
6	Моделювання та експериментальна перевірка результатів	06.11.2025-30.11.2025	Виконано
7	Охорона праці	01.12.2025-06.12.2025	Виконано
8	Охорона навколишнього середовища	07.12.2025-17.12.2025	Виконано
9	Усунення недоліків та захист кваліфікаційної роботи	18.12.2025-31.12.2025	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.т.н., доц. Катерина КАЖАН		
Охорона навколишнього середовища	д.т.н., доц. Лариса ЧЕРНЯК		

8. Дата видачі завдання: «01» вересня 2025 р.

Керівник кваліфікаційної роботи _____ Георгій КОНАХОВИЧ

(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання_____Олександр МАТВІЙЧУК-ЮДІН

(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Методи та моделі управління кіберінцидентами у кризових ситуаціях в організаціях та підприємствах критичної інфраструктури» містить 131 сторінок, 15 рисунків, 4 таблиці, 27 використаних джерел.

КІБЕРІНЦИДЕНТИ, КРИЗОВІ СИТУАЦІЇ, СТАНДАРТИЗАЦІЯ В КІБЕРБЕЗПЕЦІ, КРИТИЧНА ІНФРАСТРУКТУРА, УПРАВЛІННЯ РИЗИКАМИ, КІБЕРЗАГРОЗИ, ГРУПИ РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ, ВРАЗЛИВОСТІ, МОДЕЛІ РЕАГУВАННЯ, МОНІТОРИНГ ЗАГРОЗ, АВТОМАТИЗАЦІЯ, ПРІОРИТИЗАЦІЯ ІНЦИДЕНТІВ, РИЗИК-МЕНЕДЖМЕНТ, АДАПТИВНА МОДЕЛЬ, КОРЕЛЯЦІЯ ПОДІЙ, ОЦІНКА ВПЛИВУ, КІБЕРСТІЙКІСТЬ, ВИКОРИСТАННЯ РЕСУРСІВ, АПРОБАЦІЯ РЕЗУЛЬТАТІВ.

Об’єкт дослідження – процес реагування на кіберінциденти в організаціях критичної інфраструктури.

Предмет дослідження – методи та інструменти організації процесу реагування на кіберінциденти в умовах кризових ситуацій

Метод дослідження – Сканування трафіку мереж, виявлення порушень, аномалій за допомогою SIEM системи. Методи апробації результатів включають моделювання та симуляції в реальних умовах.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

NIST - National Institute of Standards and Technology

ISO/IEC - International Organization for Standardization / International Electrotechnical Commission

ENISA - European Union Agency for Cybersecurity

CERT - Computer Emergency Response Team

CSIRT - Computer Security Incident Response Team

SOC - Security Operations Center

NCSC - National Cyber Security Centre

SIEM - Security Information and Event Management

SOAR - Security Orchestration, Automation and Response

СУІБ - Система управління інформаційною безпекою

IDS - Intrusion Detection System

IPS - Intrusion Prevention System

CTI - Cyber Threat Intelligence

SCADA - Supervisory Control And Data Acquisition

ВСТУП

Актуальність теми. Зі зростанням кіберзагроз проблема управління кіберінцидентами набуває особливої актуальності, зокрема для підприємств критичної інфраструктури. Критична інфраструктура (КІ) - це сфера, від надійності та безперервності роботи якої залежить національна безпека, економічний добробут і життя громадян. В умовах кризових ситуацій - таких як воєнні конфлікти, техногенні аварії, енергетичні кризи - стійкість роботи об'єктів КІ визначально залежить від їхньої здатності протистояти та оперативно реагувати на кіберінциденти. Наприклад, під час війни кібератаки на енергосистеми чи урядові мережі можуть спричиняти масштабні відключення електроенергії або порушення зв'язку, що додатково дестабілізує ситуацію. Відомими є кейси виведення з ладу об'єктів інфраструктури через кібератаки: так, атака вірусу «Black Energy» на «Укренерго» у 2015 році призвела до відключення електропостачання; у 2021 році інцидент із програмою-вимагачем на американському трубопроводі «Colonial Pipeline» спричинив зупинку постачання пального та оголошення надзвичайного стану в окремих штатах США. Подібні інциденти швидко переростають у кризові ситуації, коли кібератака має не лише технічні, а й соціально-економічні наслідки.

Зв'язок роботи з науковими програмами, планами, темами.

Мета і завдання дослідження.

Мета дослідження полягає в аналізі сучасних методів, моделей управління кіберінцидентами в умовах кризових ситуацій та застосуванні оптимального комплексу моделей, які підвищать кіберстійкість критично важливих підприємств.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Здійснити аналіз визначень термінології, що пов'язана з кіберінцидентами, кризовими ситуаціями та критичною інфраструктурою, на основі міжнародних стандартів і законодавства України.

2. Дослідити міжнародні стандарти NIST, ISO/IEC, ENISA і нормативно-правову базу, що регламентує процес управління інцидентами.

3. Розглянути інституційні моделі та кращі практики взаємодії команд реагування CERT, CSIRT, SOC.

4. Сформувати на базі розглянутих моделей методологію реагування на кіберінциденти.

5. Дослідити науково-практичний досвід існуючих моделей управління кіберінцидентами, зокрема в критичних середовищах.

6. Визначити недоліки поточних підходів та сформувати вимоги до удосконаленої методології та моделі.

7. Впровадити імітаційні експлуатаційні умови функціонування систем мережевого моніторингу, валідні в умовах кризових ситуацій.

Об'єктом дослідження є процес реагування на кіберінциденти в організаціях критичної інфраструктури.

Предметом дослідження є методи та інструменти організації процесу реагування на кіберінциденти в умовах кризових ситуацій в організаціях та підприємствах критичної інфраструктури.

Академічна і практична актуальність теми зумовлена необхідністю забезпечити безперервне функціонування критичних послуг навіть за умов комплексних криз.

Кібернетичні атаки дедалі частіше використовуються як елемент гібридних воєн, терористичних актів або організованої злочинності, що підтверджується зростанням кількості інцидентів у світі за даними ENISA, 2023. Тому управління кіберінцидентами від попередження до післяінцидентного відновлення стало ключовим компонентом національних стратегій кібербезпеки.

Методологічну основу дослідження складають міжнародні стандарти та рекомендації. Зокрема, у роботі враховано положення керівництва NIST SP 800-61 Rev.2 Computer Security Incident Handling Guide, яке описує етапи реагування на інциденти. Також розглянуто стандарти серії ISO/IEC 27000, насамперед ISO/IEC 27035:2016, що встановлює процеси управління інцидентами інформаційної безпеки. Крім того, стандарти ISO/IEC 27001 та ISO/IEC 27002 приділяють увагу необхідності впровадження політик і процедур реагування на інциденти як невід'ємної складової системи управління інформаційною безпекою.

Важливими орієнтирами є рекомендації ENISA щодо побудови національних команд реагування, рамкові моделі, а також вітчизняні нормативні акти, зокрема Закон України «Про основні засади забезпечення кібербезпеки України» від 2017 року та підзаконні акти Держспецзв'язку. Сукупність цих документів формує методологічне підґрунтя для розробки моделі управління кіберінцидентами, адаптованої до українських реалій.

Методи досліджень. Сканування трафіку мереж, виявлення порушень, аномалій за допомогою SIEM системи. Методи апробації результатів включають моделювання та симуляції в реальних умовах.

Наукова новизна та практичне значення отриманих результатів.

Наукова новизна отриманих результатів:

1. Удосконалено модель підтримки прийняття рішень при реагуванні на кіберінциденти, яка, на відміну від повністю автоматизованих систем, базується на гібридному підході. автоматичний збір та кореляція подій Syslog поєднується з генерацією рекомендацій для оператора. Це дозволяє зменшити когнітивне навантаження на персонал у кризових ситуаціях та пришвидшити етап «Орієнтації» в циклі OODA.

2. Набув подальшого розвитку метод виявлення аномалій у мережевих протоколах віддаленого доступу на прикладі SSH. Новизна полягає в застосуванні розроблених правил фільтрації та агрегації лог-файлів у середовищі Graylog, що дозволяє ідентифікувати патерни атак (підбір паролів, сканування) на етапі ініціалізації з'єднання, мінімізуючи час до виявлення.

3. Запропоновано методику підвищення оперативності реагування через інтеграцію системи моніторингу із зовнішніми каналами сповіщення. Наукова складова полягає в обґрунтуванні архітектури, де критичні алерти обробляються окремим програмним модулем і доставляються відповідальним особам напряму

Практичне значення отриманих результатів:

1. Розроблено та впроваджено прототип системи централізованого логування на базі платформи Graylog, розгорнутий у віртуальному середовищі.

Система налаштована на збір даних протоколу Syslog з вузлів інфраструктури, що забезпечує збереження доказової бази інцидентів та можливість проведення ретроспективного аналізу подій безпеки.

2. Створено програмний скрипт для автоматизації процесу сповіщення, який інтегрує систему моніторингу з мобільними платформами оперативного зв'язку. Впровадження цього інструменту дозволило на практиці зменшити час реакції на критичні події, такі як масові невдалі спроби SSH-автентифікації, забезпечуючи миттєве інформування адміністратора незалежно від його перебування за робочим місцем.

3. Налаштовано спеціалізовані дашборди та правила алертінгу в середовищі Graylog для візуалізації спроб несанкціонованого доступу. Це надає адміністраторам готовий інструментарій для моніторингу в режимі реального часу, дозволяючи швидко оцінювати масштаб атаки та приймати обґрунтовані рішення щодо блокування зловмисних IP-адрес.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

1. 2024 IEEE 5th International Conference on Advanced Trends in Information Theory (ATIT) 21-23 November 2024р.

2. Міжнародна науково-практична конференція здобувачів вищої освіти і молодих учених «Політ. Сучасні проблеми науки» 2025р.

3. XI Всесвітній конгрес "Авіація в XXI столітті" 2025р.

4. CEUR Workshop Proceeding, CH&CMiGIN 2025. p

Результати дослідження пройшли практичну апробацію в середовищах, що імітують реальні експлуатаційні умови, зокрема в режимах роботи мережевого моніторингу, які валідні під час кризових ситуацій. Отримані дані підтверджують дієвість запропонованих підходів і засвідчують придатність для впровадження у практичних сценаріях.

РОЗДІЛ 1
АНАЛІЗ СУЧАСНОГО СТАНУ УПРАВЛІННЯ КІБЕРІНЦИДЕНТАМИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

1.1. Нормативно-правові засади захисту інформаційних ресурсів критичної інфраструктури

Кіберінцидент – це небажана або несподівана подія у кіберпросторі, яка може загрожувати конфіденційності, цілісності чи доступності інформаційних ресурсів або порушувати нормальне функціонування інформаційних систем [1]. Різні стандарти і організації надають свої акценти в цьому визначенні. Згідно з NIST SP 800-61 Rev.2, NIST визначає інцидент як порушення політики безпеки або успішну атаку, що ставить під загрозу інформаційні системи чи дані. Зокрема, у Федеральному законі США FISMA кіберінцидент трактується як «подія, що фактично або неминуче загрожує цілісності, конфіденційності чи доступності інформації чи інформаційної системи, або є порушенням законів чи політик безпеки».

Європейський підхід, закріплений у NIS2, 2022, визначає інцидент через призму впливу: «подія, що компрометує доступність, автентичність, цілісність або конфіденційність даних чи послуг, які пропонуються через інформаційні системи». Українське законодавство також дає системне визначення. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [2], кіберінцидент **-** це подія або ряд несприятливих подій, у тому числі ненавмисних, що створюють загрозу безпеці електронних комунікаційних систем чи систем керування технологічними процесами і можуть призвести до порушення їх штатної роботи. Таким чином, українське визначення охоплює не лише навмисні атаки, а й техногенні збої чи помилки, якщо їх наслідки загрожують інформаційній безпеці.

Порівнюючи підходи різних організацій, можна відзначити, що американський NIST фокусується на аспекті порушення політик та ознаках атаки, європейські структури ENISA, CERT-EU – на впливі події на послуги та дані, а українські норми

– на широкому спектрі причин і умов, що призводять до інциденту. ENISA в своїх глосаріях використовує визначення, узгоджені з директивами ЄС. Інцидент – це подія, що має негативний вплив на інформаційні системи чи дані, а CERT-EU як команда реагування установ ЄС трактує кіберінцидент виходячи з потенціалу завдати шкоди ІТ-інфраструктурі органів Євросоюзу. Спільним у всіх підходах є розуміння інциденту як явища, що виходить за межі штатних подій в кіберпросторі і потребує застосування заходів реагування.

Під кризовою ситуацією визначений стан, за якого нормальне функціонування системи чи організації істотно порушене, виникає загроза життєво важливим інтересам і для подолання ситуації потрібні надзвичайні заходи. У контексті кібербезпеки кризова ситуація може виникнути, коли масштабний кіберінцидент спричиняє довготривалу відмову критичних сервісів або ланцюгову реакцію з перебоями в суміжних галузях [3]. Кризовими також можна вважати ситуації, коли кібератака використовується паралельно з фізичними атаками у воєнний час, підсилюючи загальний деструктивний ефект.

Критична інфраструктура формується як сукупність секторів, об’єктів, від безперервного функціонування яких залежить національна безпека, стійкість економіки та безпека суспільства. Законодавство України визначає критично важливі об’єкти інфраструктури як підприємства, установи та організації, порушення функціонування яких може мати значний негативний вплив на національну безпеку, оборону, довкілля, економіку чи здоров’я і життя людей. До таких об’єктів належать електромережі, нафтогазовий сектор, авіація, залізничний, трубопровідний, зв’язок і цифрові послуги, фінансова система, охорона здоров’я, водопостачання тощо. В міжнародній практиці поняття критичної інфраструктури співвідноситься з терміном Critical Information Infrastructure, коли йдеться саме про інформаційні системи цих об’єктів.

Кіберінциденти на об’єктах критичної інфраструктури особливо небезпечні тим, що здатні ескалувати у повномасштабні кризові ситуації. Причиною є тісна залежність сучасного суспільства від безперервності критичних послуг. Наприклад, якщо атака на енергетичну інфраструктуру спричиняє блекаут, то наслідки

відчуваються у всіх сферах. Таких як зупинка транспорту, зв'язку, замороження роботи підприємств і потребують залучення сил цивільного захисту, що є ознакою кризи. Такий випадок стався в Україні у грудні 2015 року, коли внаслідок кібератаки було відключено частину електромережі.

Інцидент локального рівня переріс у регіональну надзвичайну ситуацію з населенням, що залишилося без електрики. В секторі транспорту прикладом може бути кібератака на інформаційні системи логістичної компанії або портового оператора. Зокрема, вірус NotPetya у 2017 році вразив глобальні мережі, паралізував роботу морських портів і порушив світові логістичні ланцюги, що спричинило значні економічні збитки [4]. У сфері державного управління показовою була атака на ланцюг поставок SolarWinds 2020 р.. Зловмисники отримали доступ до мереж численних урядових установ по всьому світу, в тому числі у США, що викликало потребу у масштабних заходах реагування на національному рівні. В Україні потенційно кризовими могли б стати атаки на цифрові державні сервіси. Прикладом є порушення роботи платформи «Дія» або реєстрів державних послуг внаслідок кібератаки суттєво вплинуло б на мільйони громадян і вимагало б невідкладного втручання держави.

Отже, кіберінцидент на об'єкті критичної інфраструктури – це не просто локальна технічна проблема, а подія, що може мати каскадний ефект і переростати у кризу. Розуміння термінів і природи таких інцидентів є відправною точкою для побудови ефективних методів управління ними.

1.2. Аналіз нормативних документів та стандартів серії NIST та ISO/IEC

Для побудови процесів реагування на інциденти залишається керівництво NIST SP 800-61 Rev.2 "Computer Security Incident Handling Guide", де процес подано як послідовність фаз: підготовка; виявлення й аналіз; локалізація, ліквідація та відновлення; діяльність після інциденту. Підготовка включає формування політик реагування, рольових матриць, каналів комунікації, сценаріїв, наборів інструментів

форензики та резервних планів. Виявлення й аналіз акцентують збір телеметрії з кінцевих точок, мережі, хмарних ресурсів і журналів застосунків, кореляцію в SIEM, тріаж оповіщень та класифікацію інцидентів за впливом і терміновістю. Фаза локалізації, ліквідації та відновлення деталізує тактики розмежування зон і сегментації, відключення уражених вузлів, видалення шкідливого ПЗ, ротацію облікових даних, відновлення з “чистих” бекапів та поступове повернення до продуктивної експлуатації з підвищеним моніторингом. Згідно з NIST SP 800-61 Rev.2, завершальна фаза передбачає ретроспективний аналіз, оновлення політик і засобів контролю, удосконалення навчання та вправ з кіберстійкості.

У 2022–2024 рр. екосистема документів NIST розвивалася в руслі узгодження процесу реагування з NIST Cybersecurity Framework (CSF) 1.1/2.0, що підкреслило необхідність інтегрувати інцидент-менеджмент у цикл ризик-менеджменту, керування активами, вразливостями та безперервністю [5]. Разом з тим, у практичному дискурсі КІ в Україні й надалі широко посилаються саме на ревізію як на перевірений довідник із чітко структурованим життєвим циклом інциденту.

Серія ISO/IEC 27035:2016 формує процесну основу управління інцидентами інформаційної безпеки. В частині 1 описано базові поняття та загальні фази процесу; в частині 2 проявлено фокус на плануванні та підготовці реагування, включно з політикою, ролями керівництва, ресурсами, навчанням і тестуванням, частини 3 деталізують спеціалізовані аспекти, залежно від редакції. Відповідно до ISO/IEC 27035:2016, методологічно ISO/IEC 27035 структурує процес як п’ять фаз. Планування і підготовка, ідентифікація та повідомлення, оцінка та прийняття рішення, реагування, навчання на досвіді. Відмінною рисою ISO-підходу є сильний акцент на інституційному врядуванні, управлінні компетенціями команди, контролі змін і документуванні, що критично для середовищ із підвищеною регуляторикою енергетики, транспорту, урядових послуг.

Суміжні стандарти ISO/IEC 27001:2022 та ISO/IEC 27002:2022 надають вимоги до і довідник контрольних заходів відповідно [6]. Для середовищ КІ це означає інтеграцію інцидент-менеджменту в ширший цикл управління ризиками, аудитів і безперервного вдосконалення, а також відображення процедур реагування в реєстрах

ризиків, політиках та планах безперервності. На практиці це забезпечує трасованість від індикаторів компрометації IoC до записів ризик-реєстру та пост-інцидентних змін у контролях, наприклад, посилення журналювання, MFA, сегментації мережі.

NIST, згідно з NIST SP 800-61 Rev.2, прагматично орієнтує організації на операційне реагування, швидке виявлення, стримування, відновлення та навчання на інциденті. ISO/IEC, відповідно до ISO/IEC 27035:2016; ISO/IEC 27001:2022, наголошує на системності й відповідності. Відповідальності керівництва, політиках, компетенціях і неперервному вдосконаленні в межах СУІБ. Обидва підходи визнають цикл підготовки, виявлення/аналізу, реагування/відновлення, уроки, однак ISO/IEC формалізує процесні та управлінські артефакти, а саме, політики, ролі, записи, компетенції, тоді як NIST детальніше описує тактико-технічні аспекти реагування, триажу та форензіки.

NIST забезпечує операційну придатність, для команд SOC/CSIRT. ISO/IEC надає сертифікаційну й управлінську рамку, яку легше вмонтувати в корпоративне врядування та регуляторні вимоги.

NIST менше фокусується на формальних вимогах до СУІБ і суміжних процесів відповідності; ISO/IEC, своєю чергою, традиційно залишає тактичні плейбуки на розсуд організації, що вимагає додаткового “операціоналізування” через локальні регламенти та SOP.

Нормативна база України визнає необхідність організувати процес реагування на інциденти відповідно до міжнародних практик. Відправною точкою є Закон України «Про основні засади забезпечення кібербезпеки України», а також підзаконні акти Держспецзв’язку, методичні матеріали CERT-UA, Державного центру кіберзахисту. На практиці оператори КІ поєднують ISO/IEC 27001/27002/27035 як сукупність вимог і контролів із рекомендаціями NIST щодо операційного інцидент-менеджменту.

1.3. Інституційні моделі взаємодії підрозділів кібербезпеки

Взаємодія підрозділів безпеки відповідно вищеописаних стандартів, будується багаторівнево. SOC забезпечує безперервний моніторинг, кореляцію подій у SIEM, оркестрацію реакцій у SOAR та первинний тріаж інцидентів. CSIRT/CERT виконує функції розслідування, координації між підрозділами/партнерами, комунікації з регуляторами, а також управління життєвим циклом інциденту від ескалації до lessons learned. На національному рівні NCSC/CERT-UA/CERT-EU координують обмін розвідданими про загрози (Рис.1.1), міжвідомчу взаємодію, попередження масштабних інцидентів і кризове управління.

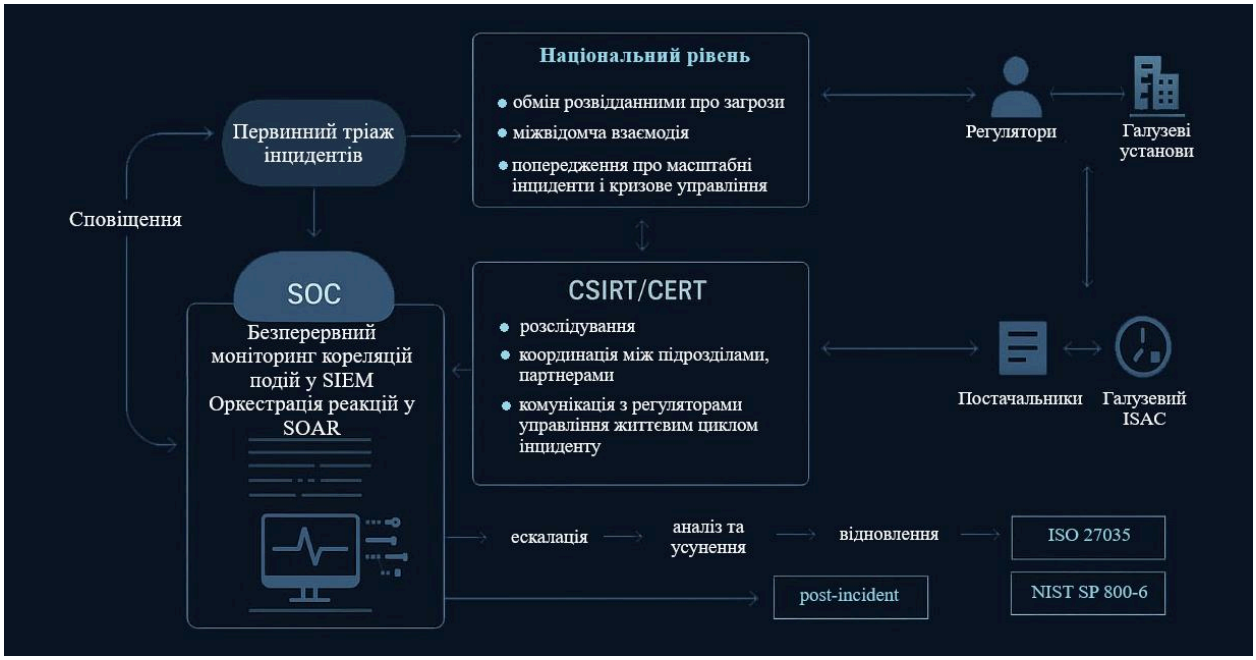

Рис. 1.1. Модель взаємодії підрозділів безпеки

У ЄС взаємодію між національними командами координує мережа CSIRTs Network під егідою ENISA та CERT-EU, що виконує роль інформаційно-координаційного вузла для інституцій ЄС. Така модель критично важлива під час крос-кордонних інцидентів на кшталт атак на ланцюги постачання або поширення шкідливого ПЗ між державами-членами [6].

В Україні політику та координацію у сфері кібербезпеки здійснює Держспецзв’язок, у складі якої функціонує Державний центр кіберзахисту та урядова

команда CERT-UA. CERT-UA забезпечує реагування на кіберінциденти, взаємодію з правоохоронними органами та міжнародними партнерами, випускає попередження та аналітичні повідомлення для суб'єктів КІ.

Практика останніх років показує сталу тенденцію до зростання кількості інцидентів і, відповідно, – до посилення операційної взаємодії з операторами КІ. На прикладному рівні оператори КІ — НЕК "Укренерго" (оператор системи передачі), група НАК "Нафтогаз України", міські/регіональні оператори енергомереж — відповідні оператори розподілу, а також платформа цифрових держпослуг "Дія", як цифрова інфраструктура державних сервісів — вибудовують моделі взаємодії з CERT-UA та профільними органами, інтегруючи власні SOC/CSIRT-процедури з національними каналами сповіщення та ескалації.

Відповідно міжнародної практики впровадження моделей реагування, можна виокремити такі впроваджені практики:

US-CERT / CISA координує реагування на національному рівні, публікує технічні директиви та спільні консультації, забезпечує обмін IoC і кращими практиками.

GOV-CERT.NL (Нідерланди) є одним з європейських піонерів у державному інцидент-менеджменті з сильною практикою сповіщення постраждалих сторін і координації в ланцюгах постачання.

На рисунку 1.2 представлено архітектуру організаційно-технічної моделі кіберзахисту, яка відображає взаємодію ключових організаційних ролей, технічних засобів та процесів забезпечення інформаційної безпеки. Модель демонструє структурну побудову системи кіберзахисту, логіку обміну даними між її компонентами та механізми реагування на кіберзагрози в умовах штатного та кризового функціонування.

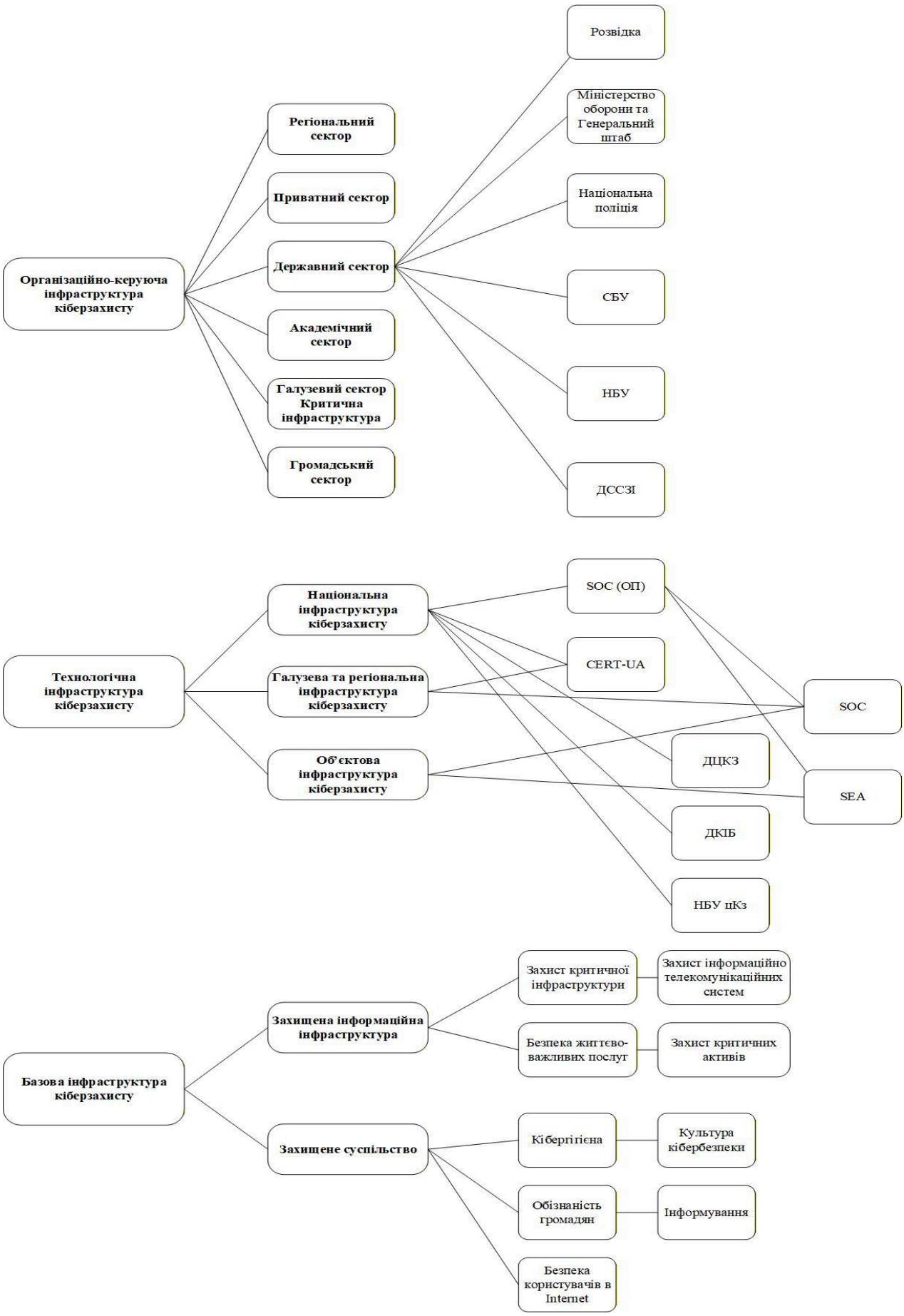

Рис. 1.2. Архітектура організаційно-технічної моделі кіберзахисту

CERT-EU (ЄС) виконує роль центра обміну та координації для інституцій ЄС, у т.ч. під час кризових подій кібератак на загальноєвропейські сервіси.

Модель плану реагування на кіберінциденти, подано на рисунку 1.3, що відображає поетапну організаційно-технічну взаємодію структурних підрозділів та відповідальних ролей у процесі управління кіберінцидентами. Модель охоплює повний цикл реагування — від планування та виявлення подій до ліквідації наслідків, інформування зацікавлених сторін і подальшого аналізу з метою вдосконалення системи кіберзахисту.

Інцидент із Colonial Pipeline 2021 р. показав, що навіть компрометація “не-операційних” систем може призвести до зупинки критичної логістики пального та регіональної кризи постачання. Реакція вимагала координації приватного оператора, федеральних структур, транспорту та енергетики.

Атака на Norsk Hydro в 2019 році продемонструвала значення прозорих комунікацій та планів відновлення: компанія тимчасово зупиняла виробництво, але завдяки відкритій комунікації та поетапному відновленню зменшила репутаційні втрати [7].

Натомість SolarWinds 2020 році висвітлив масштабність ризиків ланцюга постачання і потрібність централізованого обміну IoC між державними органами та підрядниками. Для України знаковими лишаються події 2015 року в енергетиці та хвиля NotPetya 2017 році, що уразила логістику Maersk і низку організацій у різних країнах, засвідчивши потребу в міжгалузевій та міждержавній координації.

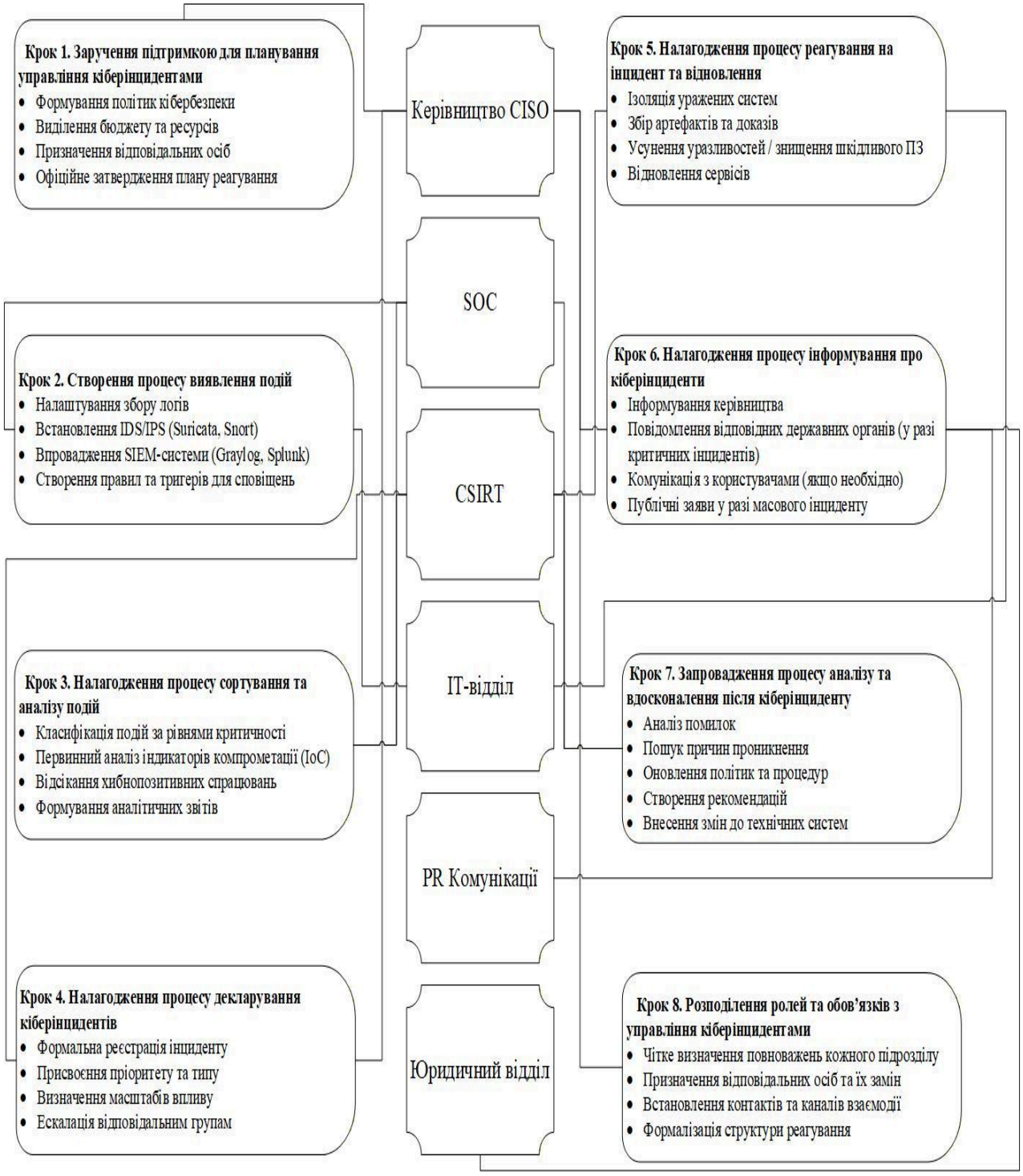

Рис. 1.3. Модель плану реагування на кіберінциденти

1.4. Наукові підходи і практичні моделі управління інцидентами

Академічні та галузеві праці часто беруть за базис життєвий цикл NIST, доповнюючи його кількісними методами пріоритетності. Наприклад, на основі впливу на безперервність критичних послуг, формальними SLA/OLA між SOC, IT-

експлуатацією та OT-підрозділами, а також метриками ефективності MTTD - середній час, необхідний для виявлення проблеми або інциденту, MTTR - середній час, необхідний для повного відновлення системи після збою. Даний підхід, поєднаний з exercise-driven development, дозволяє інституціоналізувати lessons learned (засвоєні уроки) і підвищувати кіберстійкість.

На рисунку 1.4 відображено етапність життєвого циклу кіберінциденту, яка включає послідовні фази підготовки, виявлення та аналізу, стримування, усунення й відновлення, а також дій після інциденту. Представлена модель (1.4) дозволяє систематизувати процес управління кіберінцидентами та забезпечує структурований підхід до реагування і підвищення рівня кіберстійкості організації.

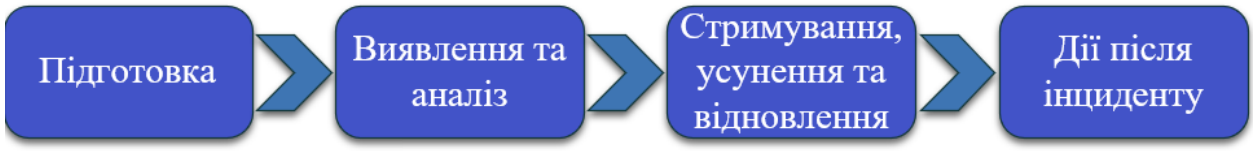

Рис. 1.4. Етапність життєвого циклу інциденту

Для вимірювання та планування розвитку функції реагування застосовують моделі зрілості. Поряд із загальними CMMI-подібними підходами (фреймворк, для вдосконалення процесів та підвищення показників ефективності в організаціях), у практиці CSIRT поширена модель SIM3 (Модель зрілості управління інцидентами безпеки), що оцінює організаційні, операційні та технічні аспекти команд реагування, включно з процесами комунікації та співпраці. За даними ENISA CSIRT, пов'язані інструменти самооцінки. Для підприємств КІ застосування таких моделей забезпечує пріоритезацію інвестицій у безпеку за принципом "від базових спроможностей до поширених автоматизацій".

Науково-практичні роботи останніх років детально аналізують детекцію на основі поведінкових ознак, кореляцію подій, машинне навчання для зменшення "шуму" оповіщень і автоматизацію рутинних кроків із контролем людини. У середовищах КІ, особливо OT/ICS ефективність досягається через гібридний моніторинг IT-/OT-мереж, де SIEM отримує події з SOC-зон, а SOAR реалізує

детерміновані плейбуки із безвідмовними механізмами для стримування інцидентів без ризику для технологічної безпеки. Важливо, що в умовах кризи, наприклад, енергетична напруга, воєнний стан, правила ескалації та канали зв'язку мають бути наперед перевірені під "пікові навантаження" і відмовостійкі.

Дослідження зосереджені на поєднанні детекції аномалій з розвідданими про загрози для динамічної адаптації плейбуків. Для КІ критична здатність оцінювати системний ризик. Наприклад, інцидент на вузлі SCADA має пріоритет над типовим фішинг-ланцюжком через потенціал фізичних наслідків [8]. Після випадків типу NotPetya та Colonial Pipeline у наукових публікаціях посилилася увага до макроскопічних моделей впливу секторальні симуляцій, теорії мереж, каскадних відмов, а також до крос-організаційної співпраці через національні/регіональні обміни IoC та спільні навчання.

Для НЕК "Укренерго" та операторів розподільчих мереж практична модель включає відокремлення OT-сегментів, моніторинг через спеціалізовані датчики ICS/SCADA, процедури ручного керування, а також інцидент-плани на випадок енергетичних блекаутів. Для НАК "Нафтогаз України" та нафто-газового сегмента актуальні сценарії ланцюгів постачання, а також захист комерційних і технологічних IT-ландшафтів. Для платформи "Дія" як цифрової інфраструктури державних сервісів пріоритетом є високодоступні архітектури, резервування каналів та захист персональних даних у відповідності з національним законодавством.

1.5. Підсумок виявлених недоліків і вимог до моделі

Ключовими недоліками у багатьох операторів КІ є процедури SOC/CSIRT для офісного IT, які не повністю інтегровані з OT/ICS-процесами, що ускладнює єдину картину ситуаційної обізнаності під час криз. SOAR-автоматизації часто не охоплюють критичні ланцюги виробництва, де потрібні спеціальні плейбуки з урахуванням фізичної безпеки. Недостатня міжвідомча координація та стандартизовані SLA з національними органами. Не всюди формалізовано канали, часові вікна та формати повідомлень до CERT/NCSC. Випадки SolarWinds/NotPetya

показали, що типові контролі не покривають транзитивні довіри до MSP/постачальників ПЗ та оновлень.

Вимогами до удосконалення моделі управління кіберінцидентами для КІ є:

- єдиний операційний каркас “IT/OT-fusion IR”;
- узгоджені плейбуки й канали ескалації для ІТ та ОТ, спільні ситуаційні панелі, а також ризик-адаптивні правила стримування з пріоритетом безпеки технологічних процесів;
- визначені SLA/OLA з CERT-UA/регуляторами, стандартизовані формати сповіщень, регулярні спільні навчання;
- оцінка впливу на бізнес/технологічні процеси для каскадних відмов, запасні режими ручного керування, спроможність до швидкого ізольованого запуску критичних вузлів [8].

Перевірка довірчих відносин, підписані оновлення, SBOM, моніторинг аномалій у CICD, сегментація з підрядниками.

ВИСНОВКИ ДО РОЗДІЛУ 1

В результаті проведеного аналізу можна констатувати, що управління кіберінцидентами для критичної інфраструктури має спиратися на поєднання операційного підходу NIST, орієнтацію на швидке й ефективне реагування та системно-керованої рамки ISO/IEC, інтеграцію в СУІБ, ролі та політики, безперервне вдосконалення. Інституційні моделі ЄС та України ENISA, мережа CSIRTs, CERT-EU, CERT-UA доводять важливість централізованої координації, обміну розвідданими про загрози, стандартизованих каналів ескалації та спільних навчань. Випадки з Colonial Pipeline, Norsk Hydro, SolarWinds, NotPetya, енергосектор України 2015 показали, що інциденти в КІ можуть швидко ескалувати до кризових ситуацій з матеріальним впливом на економіку та добробут населення, а тому процес інцидент-менеджменту має бути секторально адаптованим, міжвідомчо узгодженим і постійно тренованим.

Таким чином, ключовою задачею наступного розділу є конструювання удосконаленої моделі, що усуває ідентифіковані прогалини, зшиває IT/OT-процеси, формалізує крос-організаційні SLA з національними органами, підсилює автоматизації SOAR у межах безпечних для виробництва сценаріїв і встановлює прозорі метрики ефективності.

РОЗДІЛ 2
КЛАСИФІКАЦІЯ ТА ІДЕНТИФІКАЦІЯ ЗАГРОЗ І ВРАЗЛИВОСТЕЙ У КРИТИЧНІЙ ІНФРАСТРУКТУРІ

2.1. Класифікація загроз за галузевими доменами

Критична інфраструктура охоплює галузі, від стабільності яких залежить національна безпека, економіка та життя громадян. Згідно з міжнародною практикою та національними нормативами України, до критичної інфраструктури належать сектори енергетики, транспорту, телекомунікацій, фінансового сектору, охорони здоров'я, водопостачання і державного управління. Кожен із цих доменів має власні особливості та типові кібератаки. Військовий конфлікт 2022–2024 років значно підвищив кількість і різноманітність кібератак на критичну інфраструктуру України.

В енергетиці головну небезпеку становлять атаки на системи управління технологічними процесами ICS/SCADA, зловмисне програмне забезпечення, здатне порушити подачу електроенергії, а також вимагальне ПЗ, що паралізує ІТ-системи енергокомпаній. У транспортній галузі актуальними є атаки на ІТ-інфраструктуру перевізників та можливе втручання в роботу систем управління рухом [9]. Для телекомунікацій характерні потужні DDoS-атаки на мережеві вузли та сервери провайдерів, що викликають масштабні збої в інтернет- та телефонному зв'язку, а також атаки на супутникові мережі зв'язку. Фінансовий сектор регулярно зазнає DDoS-атак на веб-сайти банків і платіжні системи для підриву довіри та доступності сервісів. Крім того, фінансові установи наражаються на шпигунські та деструктивні атаки, а також на цілеспрямоване розкрадання коштів через компрометацію SWIFT та інші шахрайські операції.

У сфері охорони здоров'я найнебезпечнішими є атаки-вимагання на госпітальні ІТ-системи, що призводять до блокування доступу до медичних даних, зупинки роботи обладнання та загрози життю пацієнтів. Так, глобальна атака WannaCry 2017 року паралізувала роботу третини лікарень Англії, спричинила перенаправлення

швидких та скасування близько 19 тисяч прийомів пацієнтів. Для систем водопостачання характерні загрози з боку кіберсаботажу: зловмисники можуть отримати несанкціонований віддалений доступ до SCADA водоканалів і змінити параметри хімічної обробки води або вивести з ладу насосне обладнання. У 2023–2024 рр. український CERT фіксував діяльність російської групи Sandworm, яка впроваджувала шкідливі програми та вайпери у мережі підприємств водопостачання, намагаючись знищити критичні дані. У сфері державного управління найтиповіші загрози – це дефейс і виведення з ладу вебресурсів, масовані DDoS на державні сервіси та кібершпигунство. Характерний приклад – у січні 2022 року хакери атакували близько 70 урядових сайтів України, одночасно в мережі державних органів було поширено деструктивне ПЗ-вайпер для знищення даних. Ця атака була частиною тактики «гібридної війни» перед відкритим вторгненням. У таблиці 2.1 зведено класифікацію загроз за доменами із зазначенням типу загрози, механізму реалізації та конкретного кейсу.

Таблиця 2.1

Класифікація кіберзагроз за галузевими доменами критичної інфраструктури

Галузевий домен	**Приклади критичних систем**	**Характерні кіберзагрози**
Енергетика	Електромережі (SCADA/ICS-системи), нафто- і газопроводи, електростанції	Цілеспрямовані атаки APT на системи керування технологічними процесами, віруси-вимагачі, DDoS-атаки на сервіси енергокомпаній, компрометація постачальників.
Транспорт	Залізничні системи керування, авіаційні навігаційні системи, морські порти та логістичні системи	Злам систем диспетчеризації, кібератаки на авіаційні бази даних і системи планування польотів, GPS-спуфінг та глушіння сигналів, шкідливі програми, що вражають логістичні шляхи.

Закінчення таблиці 2.1

Комунікації	Мережі інтернет-провайдерів, телекомунікаційні вузли, центри обробки даних, супутниковий зв'язок	Масові DDoS-атаки на вузли зв'язку та веб-портали, злам обладнання мереж, атаки на супутникові мережі, знищення волоконно-оптичних магістралей або радіорелейних станцій у поєднанні з кібератаками
Фінансовий сектор	Банківські IT-системи, платіжна інфраструктура (банкомати, POS), біржові платформи	Кібершпигунство та фінансові APT, крадіжки коштів через злам SWIFT-терміналів, віруси типу wiper та ransomware, DDoS на онлайн-банкінг.
Охорона здоров'я	Лікарняні інформаційні системи, системи управління обладнанням, швидка допомога	Програми-вимагачі, що шифрують медичні дані та виводять з ладу госпітальні системи, крадіжка та витік персональних даних пацієнтів, атаки на медичні IoT-пристрої, що можуть поставити під загрозу життя хворих.
Державне управління	Портали електронних послуг, реєстри державних даних, урядові відомчі мережі	Злам державних веб-сайтів, викрадення конфіденційних даних урядових установ шляхом шпигунського ПЗ, проникнення в електронні реєстри з метою зміни чи знищення даних, DDoS-атаки на інформаційні ресурси органів влади для підриву їх доступності, компрометація облікових записів державних службовців для доступу до внутрішніх мереж.

У таблиці 2.1 показано, що DDoS-атаки є універсальною загрозою для багатьох доменів – зокрема фінансового, державного, телеком- і транспортного секторів. Їхня мета – підірвати доступність сервісів через масове перевантаження мережі запитами. Наприклад, у лютому 2022 р. зафіксовано серію DDoS на сайти Міністерства оборони та провідних банків України, які США та Велика Британія приписали російським військовим хакерам. Іншим розповсюдженим типом загроз є вимагальне програмне забезпечення, ransomware, яке особливо небезпечне для медичної та енергетичної сфери. Напади на лікарні з шифруванням даних створюють пряму загрозу життю людей і можуть мати тяжкі наслідки. За даними ENISA, у 2021–2023рр. 54%

інцидентів у секторі охорони здоров’я становили саме атаки ransomware. В енергетиці і промисловості дедалі більшої ваги набувають цілеспрямовані атаки на операційні технології. На відміну від IT-систем, OT-контролери та SCADA пов’язані з фізичними процесами, тому їх компрометація може призвести до аварій і відключень. Зафіксовано кілька руйнівних кібератак на енергетику України. У 2015 та 2016рр. атаки BlackEnergy та Industroyer призвели до вимкнення електропостачання в частині регіонів. У квітні 2022р. під час війни російська група Sandworm здійснила нову спробу – впровадила модернізований malware для відключення кількох підстанцій високої напруги, одночасно запустивши вайпери для ускладнення відновлення [10].

Одною з критичних типів загроз є атака на ланцюги постачання, які є вразливою одразу для кількох доменів. Зловмисники намагаються проникнути в мережі критичних підприємств через уразливості у програмному забезпеченні постачальників або обладнанні підрядників. За даними CERT-UA, у 2023р. зафіксовано неодноразові компрометації інфраструктури об’єктів енергетики, теплокомуненерго та водоканалів шляхом експлуатації бекдорів, залишених у обладнанні сторонніх постачальників, в програмованих радіомодулях SDR. Це підтверджує, що межі між IT- і OT-безпекою стають дедалі умовнішими, а атаки мають комплексний характер. Зокрема, військові кібероперації РФ 2022–2023рр. часто поєднували кібератаки з кінетичним впливом. Спочатку здійснювались проникнення у мережі критичних служб енергетики, зв’язку, держуправління для шкідливих програм бекдорів, а під час ракетних ударів ці програми активувалися для максимізації руйнувань. Таким чином, класифікація загроз за доменами показує різноманітність сценаріїв – від простих DDoS до складних багатоетапних кібератак із використанням APT-інструментів. Надалі, для успішного захисту, кожен суб’єкт критичної інфраструктури повинен ідентифікувати найбільш актуальні для нього типи загроз і врахувати їх у своїй системі кібербезпеки.

2.2. Методи виявлення вразливостей

Ефективне виявлення вразливостей є передумовою попередження кібератак. Під вразливостями розуміють слабкі місця в програмному або апаратному забезпеченні, процесах чи налаштуваннях, які можуть бути експлуатовані зловмисниками. Методи їхнього виявлення включають як проактивні заходи сканування, тестування на проникнення, так і моніторинг подій безпеки у режимі реального часу. У цьому підрозділі розглянуто основні підходи пентестування, сканування вразливостей, системи виявлення та запобігання вторгнень, аналіз журналів і кореляція подій за допомогою SIEM, а також використання розвідданих про загрози Threat Intelligence [11]. Окремо висвітлено роль центрів моніторингу безпеки у своєчасному виявленні інцидентів і наведено стандарти, що регламентують ці процеси, зокрема, ISO/IEC 27005, NIST SP 800-30.

Тестування на проникнення, пентестинг – це метод етичного злому, при якому уповноважені експерти імітують дії хакерів, намагаючись проникнути в систему для виявлення її слабких місць. Пентести можуть бути чорного ящика, тестери не мають попередньої інформації про систему, сірого ящика, часткова інформація, або білого ящика з повно. інформацією. Метою є виявлення вразливостей спробою реально їх експлуатувати, з подальшим наданням звіту та рекомендацій щодо усунення знайдених недоліків.

Пентест охоплює технічні вектори вразливості веб-додатків, мережевих сервісів, систем автентифікації і соціальну інженерію. Методики пентесту детально описані в стандартах, зокрема в NIST SP 800-115 та в Open Source Security Testing Methodology Manual. Проведення регулярних контрольованих атак дозволяє підприємствам критичної інфраструктури проактивно виявляти найнебезпечніші дірки в захисті до того, як ними скористаються зловмисники.

На додаток або на заміну ручному тестуванню використовується автоматичне сканування за допомогою спеціалізованих програм. Сканери OpenVAS, Nessus, QualysGuard містять бази знань про тисячі відомих вразливостей CVE і методично перевіряють системи на їх наявність. Процес сканування полягає у відправленні на

цільовий хост різних тестових запитів і аналізі відповідей. Nmap здійснює пошук відкритих портів і визначає версії сервісів, після чого ці версії звіряються з базою відомих вразливостей [12].

Сканери можуть виявити недостатньо оновлене ПЗ, неправильні конфігурації, відсутність шифрування, використання стандартних паролів, відомі бекдори. За даними звіту CERT-UA за 2021р., із понад 2000 вивчених кібератак значна частина стала можливою через використання вразливостей, для яких були випущені виправлення, але вони не були оперативно застосовані адміністраторами. Таким чином, регулярне сканування та оперативний патч-менеджмент є критично важливими для безпеки інфраструктури. Результати сканування вразливостей часто оформлюються у вигляді звіту з рейтинговою оцінкою ризику. Для кожної знайденої проблеми, що дозволяє пріоритизувати усунення.

Приклади типових вразливостей та інструментів їх виявлення наведено у вигляді таблиці 2.2. У таблиці перераховано поширені слабкі місця інформаційних систем, які є актуальними для об’єктів критичної інфраструктури, з зазначенням методів виявлення і джерел, в яких ці уразливості описано або було зафіксовано їх експлуатацію.

Таблиця 2.2

Приклади вразливостей та методи їх виявлення у системах критичної інфраструктури

Метод / засіб	**Призначення**	**Типові інструменти / підходи**	**Примітка**
Penetration Testing (пентест)	Імітація реальних атак для виявлення вразливостей «як зловмисник».	Методи етичного хакінгу, збір інформації OSINT, сканування портів, експлуатація Metasploit, пост-експлуатація.	Проводиться вручну або з мін. автоматизацією; на виході – звіт з рекомендаціями. Вимагає експертних знань, дає глибоке розуміння стану безпеки.
Vulnerability Scanning (сканування вразливостей)	Автоматизований пошук відомих вразливостей у системах.	Сканери *OpenVAS, Nessus, Qualys*. Відповідність базам CVE, відкриті порти.	Дозволяє швидко оцінити багато систем. Сліпе місце – 0-day. Рекомендується виконувати регулярно (щомісяця/щоквартально).

Закінчення таблиці 2.2

IDS / IPS (системи виявлення / запобігання вторгнень)	Моніторинг мережевого трафіку та подій для виявлення ознак атак; у випадку IPS – блокування атак в реальному часі.	Моніторинг мережевого трафіку та подій для виявлення ознак атак; у випадку IPS – блокування атак в реальному часі.	Ключова частина “динамічного захисту”. Ефективність залежить від актуальності сигнатур і налаштування, щоб мінімізувати false positives.
SIEM (центр. моніторинг подій безпеки)	Збір логів з різних джерел, їх кореляція і аналіз для виявлення інцидентів.	Збір логів з різних джерел, їх кореляція і аналіз для виявлення інцидентів.	Дає цілісну картину стану безпеки. Часто інтегрується з Threat Intelligence (автопошук IoC в логах). Може генерувати великий потік оповіщень – потребує кваліфікованого персоналу для аналізу.
Threat Intelligence (кіберрозвідка та обмін IoC)	Збір інформації про актуальні зовнішні загрози; проактивне попередження щодо нових атак.	Збір інформації про актуальні зовнішні загрози; проактивне попередження щодо нових атак.	Допомагає оновлювати засоби захисту «на випередження». Потребує аналізу, щоб відсіювати нерелевантні дані. Вимагає налагоджених процесів інтеграції IoC в захисні системи (наприклад, блокування на фаєрволі відомих шкідливих IP).
SOC та інцидент-реагування	Централізоване управління всіма переліченими засобами, цілодобовий моніторинг та реагування.	Централізоване управління всіма переліченими засобами, цілодобовий моніторинг та реагування.	Дозволяє оперативно реагувати на складні атаки, мінімізувати шкоду. SOAR може автоматично виконувати рутинні дії (відключити обліковку, запустити скрипт на ізоляцію хоста), що важливо в умовах браку часу під час кризи.

Різні типи вразливостей потребують різних засобів виявлення. Простим прикладом виявлення є незмінений заводський пароль адміністратора. Таку прогалину може виявити або сканер вразливостей, або навіть аудит безпеки вручну. Натомість складні логічні уразливості SQL-ін’єкції у внутрішньому веб-додатку

частіше знаходять шляхом спеціалізованого тестування DAST-сканери чи пентестери.

Для моніторингу мережевого трафіку в режимі реального часу широко застосовуються IDS системи виявлення вторгнень. Вони аналізують потік даних і шукають підозрілі шаблони, сигнатури відомих атак або аномальні відхилення від нормально поведінки. Популярні відкриті рішення – Snort, Suricata, які використовують набори правил, правила для відомих експлойтів, сканувань, шкідливого трафіку. При спрацюванні сигнатури IDS генерує сповіщення для операторів SOC.

Розвиненіші системи IPS не лише виявляють, а й автоматично блокують зловмисний трафік. Suricata в режимі IPS може відкидати пакети, що відповідають відомим атакам на протокол RDP або SQL Slammer. IDS/IPS є важливим інструментом захисту мереж критичної інфраструктури, особливо на рівні периметра та між IT і OT-сегментами. Однак їх ефективність залежить від актуальності сигнатур, система потребує регулярних оновлень баз та правильного налаштування, щоб зменшити помилкові спрацьовування [13].

Якщо IDS/IPS слідкують переважно за мережевим трафіком, то SIEM агрегує інформацію з журналів операційних систем, серверів, прикладних програм, мережевого обладнання, баз даних, антивірусів. SIEM-платформа централізовано збирає логи, зберігає їх для історичного аналізу, та здійснює кореляцію подій за наперед визначеними правилами або з допомогою алгоритмів машинного навчання. Кореляція означає зв’язування розрізнених на перший погляд сигналів у єдиний інцидент: наприклад, SIEM може зіставити подію входу під обліковим записом адміністратора з незвичної IP-адреси і майже одночасне відключення антивірусу на кількох серверах і згенерувати інцидент високого ризику.

Візуалізація у вигляді дешбордів дозволяє аналітикам SOC швидко побачити аномалії. Наприклад, різке зростання кількості відмов у доступі чи трафіку на нестандартний порт. Правильно розгорнутий SIEM значно підвищує загальну ситуаційну обізнаність про стан кібербезпеки мережі. За умови якісної конфігурації, SIEM допомагає не лише виявляти атаки, що відбуваються, але й розслідувати

інциденти завдяки аналізу логів та відповідати вимогам регуляторів щодо зберігання аудиту подій.

Важливо врахувати, що продуктивність SIEM залежить від чітко визначених правил кореляції та фільтрації. Без належного налаштування існує ризик отримати лавину помилкових позитивів або, навпаки, пропустити реальну атаку через занадто загальні правила. Тому впровадження SIEM має супроводжуватися розробкою сценаріїв моніторингу під конкретні загрози, актуальні для організації. Наприклад, для енергокомпанії буде актуальним сценарій “неочікуване перепрограмування RTU-контролера” або “зміна конфігурації реле”, тоді як банку – “масова зміна паролів користувачів” чи “одночасний логін одного користувача з двох країн”.

Cyber Threat Intelligence – це процес збирання, аналізу та застосування даних про кіберзагрози, атакувальників та їх методи для покращення захисту організації. Дані CTI можуть надходити з відкритих джерел, відгалужених від розслідувань інцидентів, від галузевих центрів обміну інформацією чи комерційних провайдерів. Типовий продукт CTI – це Indicator of Compromise, індикатор компрометації. IP-адреса серверу керування malware, хеш вірусу, домен фішингового сайту. Інтеграція таких індикаторів у SIEM/IDS дозволяє швидко виявляти відомі загрози звернення до командних серверів, які використовуються APT-групами [14].

Розвідка загроз включає й тактичний та стратегічний рівень. Аналіз тактик, технік і процедур противників, профілі APT-груп, прогнозування нових методів атак. Наприклад, використання фреймворку MITRE ATT&CK допомагає співвіднести виявлені дії з конкретними техніками та отримати підказки, з якою групою чи malware можна пов’язати цю активність. На практиці у критичній інфраструктурі впроваджуються платформи Threat Intelligence, які агрегують та автоматично розсилають оновлення про загрози до засобів захисту, таких як платформа MISP, Anomali. Також в рамках державно-приватного партнерства рекомендується участь у галузевих обмінах інформацією про кіберінциденти. Наприклад, для об’єктів енергетики – через CERT-UA або міжнародні ISAC.

Сучасні організації, особливо ті, що опікуються критичною інфраструктурою, вибудовують Security Operations Center – командний центр моніторингу і реагування.

SOC може бути внутрішнім або аутсорсинговим, але виконує спільні функції цілодобового нагляду за системами, аналізом інцидентів, координацією дій з реагування. У SOC зазвичай працюють аналітики різних рівнів.

Аналітики 1 рівня спостерігають за консоллю SIEM, фільтрують та ескалують сповіщення. Аналітики 2 рівня детально розслідують підтверджені інциденти, визначають масштаб компрометації, запускають процес реагування. Аналітики 3 рівня, експерти з загроз, здійснюють глибокий аналіз шкідливого коду, виконують проактивний пошук прихованих загроз в інфраструктурі, оцінюють уразливості та проводять пентести для покращення захисту. SOC-менеджер координує роботу команди, розставляє пріоритети та відповідає за зв'язок з керівництвом і, за потреби, з правоохоронними органами [15].

Наявність ефективного SOC довела свою користь: за оцінками IBM, компанії з розгорнутими можливостями моніторингу та автоматизації інцидентів скорочують середній час виявлення й реагування на загрози більш ніж на 100 днів. Для критичної інфраструктури, де кожна хвилина простою чи витоку може спричинити величезні збитки або загрозу життю, швидкість і злагодженість SOC є вирішальними.

На міжнародному рівні існують стандарти і рекомендації, що визначають підходи до управління вразливостями та ризиками. Стандарт ISO/IEC 27005:2018 надає керівництво з менеджменту інформаційних ризиків, зокрема наголошує на необхідності ідентифікації вразливостей, що можуть бути експлуатовані загрозами. ISO 27005 описує процес оцінювання ризиків, який починається з визначення контексту, ідентифікації активів, загроз та вразливостей, далі – аналізу й оцінки ризиків для ухвалення рішень щодо обробки ризику. Методики оцінки вразливостей можуть бути як проактивними так і реактивними. Рекомендації NIST SP 800-30 наголошують, що оцінка ризику має враховувати ймовірність загроз і потенційні уразливі місця системи та відповідні наслідки їх експлуатації. Цей документ формує основу для побудови процедур ризик-менеджменту у федеральних установах США, які також застосовні й у критичній інфраструктурі.

В Україні Держспецзв'язку (ДССЗЗІ) розробила методики аналізу стану кібербезпеки та оцінювання ризиків для інформаційно-телекомунікаційних систем

об’єктів критичної інфраструктури. Наказом Адміністрації ДССЗЗІ № 606 від 08.10.2021 затверджено Методику оцінювання стану кібербезпеки, яка серед іншого регламентує порядок обстеження систем на наявність невиправлених вразливостей та визначення пріоритетів щодо усунення тих чи інших недоліків. Загальною вимогою нормативів є періодичність. Процеси управління уразливостями повинні бути постійними та повторюваними. Це означає, що сканування і тестування безпеки мають проводитися регулярно, а нові вразливості оцінюватися без зволікань після їх публікації.

Отже, дана організація методів виявлення вразливостей від людського фактору до автоматизованих систем забезпечує багаторівневе покриття. У критичній інфраструктурі бажано використовувати комбінований підхід. Сканери та моніторингові системи для широкого охоплення і оперативності, а ручне тестування та експертний аналіз для поглибленого аудиту і виявлення складних, нестандартних проблем. При цьому успішність програм виявлення вразливостей значною мірою залежить від підтримки керівництва та дотримання стандартів, що гарантують системність та повноту такого виявлення.

2.3. Аналіз загроз в кібербезпеці

Після ідентифікації вразливостей і подій, наступним кроком є аналіз загроз. Процес оцінки, які загрози існують для системи, наскільки вони небезпечні і яким способом можуть реалізуватися. Поняття аналізу загроз тісно пов’язане з моделюванням загроз, побудовою моделі потенційного противника, його мотивів, цілей та можливих шляхів атаки на конкретну систему. Аналіз загроз дозволяє проактивно виявити, що і як атакуючий може зробити, та вжити превентивних заходів. Окрема увага приділяється сучасним трендам застосуванню штучного інтелекту для детектування загроз та ролі кіберрозвідки у прогнозуванні атак.

Метод STRIDE є одним з перших і найпоширеніших методик моделювання загроз, розроблена в Microsoft. Назва є акронімом з шести категорій потенційних загроз. Spoofing (підроблення особи), Tampering (підміна даних), Repudiation

(відмовлення від дій), Information Disclosure (розголошення інформації), Denial of Service (відмова в обслуговуванні) та Elevation of Privilege (підвищення привілеїв). Метод STRIDE застосовується під час проектування системи для кожного компонента або процесу моделюються загрози за шістьма переліченими типами [16].

Наприклад, для веб-сервера моделюються S – чи може зловмисник видати себе за легітимного користувача; T – чи може змінити передані або збережені дані; R – чи може заперечити факт своїх дій; I – які дані може витекти при компрометації; D – як можна зробити сервіс недоступним; E – чи є можливість локальному користувачу стати адміністратором через уразливість.

Використовуючи STRIDE (Рис. 2.1), розробники отримують систематизований список загроз і можуть запровадити відповідні контрзаходи ще на етапі дизайну додаванням автентифікації повідомлень, шифрування, журналювання дій.. STRIDE здебільшого має якісний характер, він не визначає пріоритет чи ймовірність загрози, лише її наявність або відсутність. Для оцінки ризику кожної знайденої загрози часто залучають інші методи, такі як рейтинги DREAD або ризикові матриці.

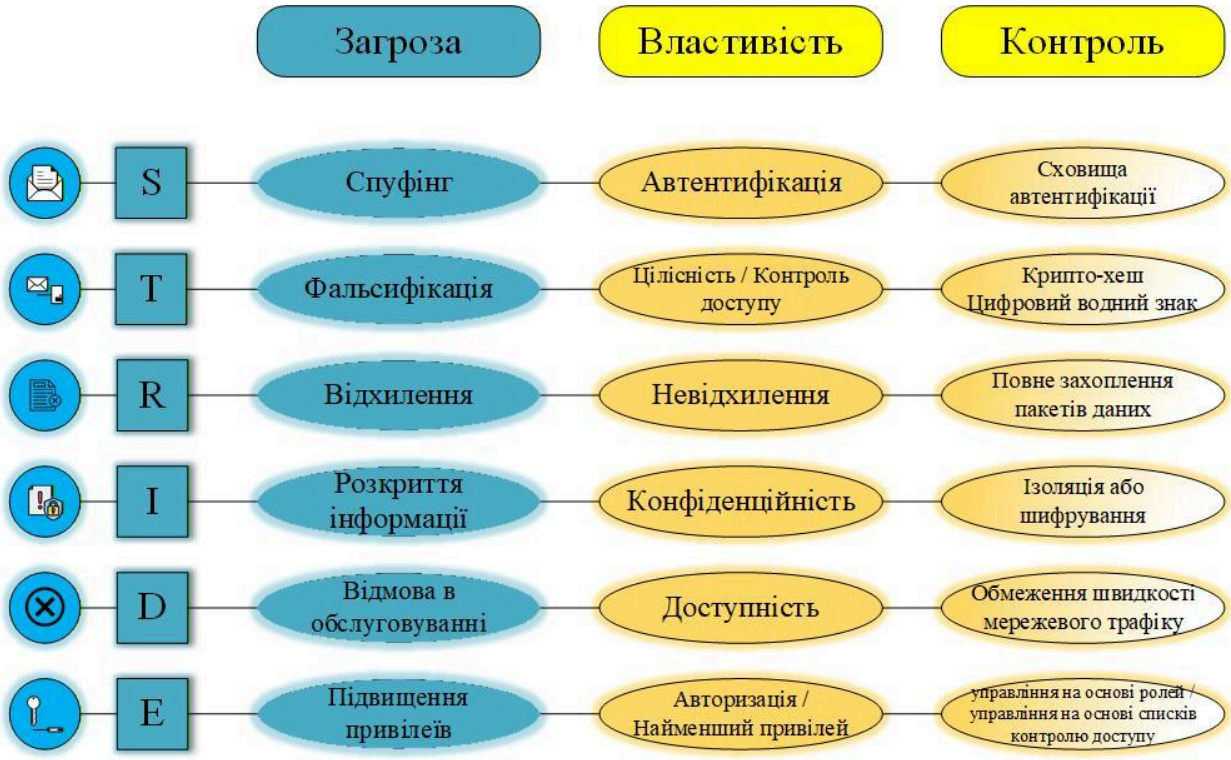

Рис. 2.1. Модель виявлення загроз за методом STRIDE

DREAD – це методика кількісного оцінювання ризику загрози, зазвичай використовується у парі зі STRIDE. Після того як перелік загроз і вразливостей ідентифіковано за STRIDE, моделі DREAD присвоює кожній загрозі п’ять оцінок. Потенційний збиток, відтворюваність атаки, складність експлуатації, частка користувачів, які постраждають і ймовірність виявлення вразливості. Кожен параметр оцінюється за шкалою від 1 до 10, потім підсумовується і виводиться середнє значення – інтегральний рейтинг ризику загрози. На практиці DREAD допомагає впорядкувати список загроз за пріоритетністю, чим вищий бал – тим першочерговіше слід усувати відповідну вразливість або впроваджувати захист. Натомість уразливість, що потребує унікальних умов і дає незначний ефект, може мати низький бал [16].

Методика PASTA це більш поглиблена, ризик-орієнтована методика моделювання загроз. Дана методика пропонує 7 етапів аналізу, що охоплюють як бізнес-аспекти, так і технічні деталі системи. PASTA має етапи визначення цілей аналізу, визначення технічної межі, декомпозиція додатку, аналізу загроз, аналізу вразливостей і слабких місць, моделювання атак, аналіз ризику та впливу. Метод PASTA фокусується на перспективі атакувальника та тісно пов’язує технічні знахідки з бізнес-наслідками, що важливо для критичної інфраструктури. Хоча PASTA є ресурсоємною методикою, її використання виправдане для систем з високими вимогами до безпеки: цей підхід дозволяє не тільки перерахувати загрози, але й випробувати можливі атаки в уявному сценарії, щоб зрозуміти, де саме лежить найбільший ризик.

Матриця загроз MITRE ATT&CK (Табл. 2.2) структурує інформацію про тактики, етапи та техніки кібератак, підтверджені реальними спостереженнями. ATT&CK подає дані у вигляді матриць. Найвідоміша матриця, що включає наразі 14 тактик, від початкового доступу до деструктивного впливу і сотні технік з унікальними ID. Кожна техніка містить опис, приклади використання APT-групами, а також поради щодо детектування і захисту [17].

Інтеграція MITRE ATT&CK в процес аналізу загроз відбувається під час розслідування інциденту чи моделяції потенційної атаки, вона може класифікувати

дії противника за відповідними техніками з ATT&CK. Це дає спільну мову для обговорення загроз і можливість закрити прогалини в безпеці. Якщо, в моделі безпеки не враховувався етап Privilege Escalation, то ATT&CK покаже конкретні техніки, які варто врахувати. Крім того, ATT&CK широко використовується для побудови технічних сценаріїв навчань, беруться декілька технік з матриці і перевіряється, чи здатні наявні засоби захисту їх виявити та зупинити. ATT&CK стала фактичним стандартом опису поведінки зловмисників, і багато виробників засобів безпеки інтегрували її в свої продукти для маркування сповіщень за відповідними техніками.

Таблиця 2.3

Фрагмент матриці загроз MITRE ATT&CK

Розвідка	**Розвиток ресурсів**	**Початковий доступ**	**Виконання**	**Закріплення**	**Підвищення привілеїв**
T1567 Ексфільтрація через веб-сервіс	T1568 Динамічна резолюція (DNS)	T1060 Ключі автозапуску в реєстрі	T1503 Облікові дані з браузерів	T1562.001 Вимкнення або зміна засобів захисту	T1098 Маніпуляції з обліковими записами
T1596 Пошук у відкритих тех. базах	T1589 Збір даних про особу жертви	T1553 Підрив довірених засобів керування	T1466 (Невідомий ID / Помилка)	T1586.001 Акаунти в соцмережах	T1021 Віддалені служби

Закінчення таблиці 2.3

T1587 Розробка можливостей	T1205 Сигналізація трафіку	T1505 Компоненти серверного ПЗ	T1566.001 Спірфішинг із вкладенням	T1021.001 Протокол RDP	T1129 Завантаження спільних модулів
T1593 Пошук на відкритих сайтах	T1335 (Ймовірно помилка або Mobile)	T1543 Створення/зміна системних процесів	T1558.003 Kerberoasting (Атака на квитки Kerberos)	T1021.002 SMB / Адмін. ресурси Windows	T1021 Віддалені служби
T1583 Придбання інфраструктури	T1590 Збір даних про мережу жертви	T1578 Невідомий ID / Помилка	T1538 Панель керування хмарним сервісом	T1041 Ексфільтрація через C2-канал	T1454 Шкідливі SMS

Станом на 2023–2025рр. відзначається стрімке впровадження технологій штучного інтелекту для виявлення й аналізу загроз. Методи Machine Learning (ML) використовуються у рішеннях класу UEBA (User and Entity Behavior Analytics) для побудови поведінкових профілів користувачів і пристроїв та пошуку відхилень, що можуть свідчити про компрометацію. Такі системи можуть самостійно вивчити, як зазвичай поводиться кожен користувач чи сервіс, і сигналізувати, якщо спостерігається нетипова активність. Штучний інтелект також допомагає зменшити навантаження на аналітиків SOC: алгоритми обробки природної мови NLP можуть аналізувати текстові описи загроз, класифікувати інциденти; нейромережі можуть автоматично категоризувати зразки шкідливого ПЗ за сімействами [18].

Якщо раніше обмін інформацією про загрози був локалізованим, то зараз він став необхідністю. Особливо це стосується критичної інфраструктури під час війни: Україна створила багаторівневу систему кібероборони, що поєднує державні структури (CERT-UA, Держспецзв'язку), волонтерське співтовариство (IT-армія) та міжнародну підтримку.

Обмін даними про нові віруси, IP-адреси атакувальників, тактики російських APT-груп дозволив значно підвищити стійкість до ворожих кампаній. Кіберрозвідка також усе частіше включає освіту персоналу: проведення тренінгів щодо актуальних загроз, внутрішні розсилки з описом нових схем фішингу тощо. Адже людський фактор залишається критичним: кращі антивіруси не допоможуть, якщо співробітник сам запустить шкідливий файл. Тому аналіз загроз – це не тільки технічна, а й організаційна задача: потрібно не лише знати про загрозу, а й донести цю інформацію до тих, хто може бути мішенню (наприклад, попередити фінансовий відділ про нову хвилю шахрайських «листів від керівника»).

Підсумовуючи вищевикладений аналіз загроз слугує поєднанням виявлення вразливостей, що потрібно захистити та управління ризиками, які потрібно усунути.

2.4. Моделі оцінки впливу та ймовірностей появи кіберінцидентів

Кіберризик традиційно визначається як поєднання двох компонентів: ймовірності настання певного кіберінциденту та величини шкоди (впливу) від нього. Для кількісного або якісного вимірювання цих складових розроблено низку моделей оцінки ризиків. Вибір моделі залежить від доступних даних, культури ризик-менеджменту в організації та вимог регуляторів. У цьому підрозділі розглянемо: прості якісні шкали (ризик-матриці), систему бальної оцінки вразливостей CVSS, рамку кількісного аналізу FAIR, а також підхід на основі байєсових мереж.

На прикладі підприємства енергетичного сектору побудуємо матрицю оцінки ризиків з урахуванням критеріїв впливу на конфіденційність, цілісність, доступність, фінансових втрат та репутації. Також звернемо увагу на практики, застосовувані у

критичній інфраструктурі: американський NIST RMF, міжнародний стандарт ISO/IEC 27005 та методичні рекомендації Держспецзв'язку України.

Якісна оцінка ризиків і матриця ризику. Найбільш поширеним підходом у менеджменті ризиків є використання якісних категорій для ймовірності та впливу. Наприклад, ймовірність події може класифікуватися як низька, середня, висока (або з додатковими градаціями – "рідко", "можливо", "майже неминуче" тощо). Аналогічно вплив (конфіденційність, цілісність, доступність, фінанси, репутація) може ранжуватися від незначного до катастрофічного. Матриця ризику будується як двовимірна таблиця: по одній осі - ймовірність, по іншій - вплив. Кожна клітинка матриці відповідає комбінації цих факторів і позначається рівнем ризику (наприклад, кольоровим кодом: зелений - низький, жовтий - середній, червоний - високий). Матриці можуть бути 3×3, 4×4, 5×5 – залежно від потрібної градації.

CVSS - оцінка критичності вразливостей. Одним із загальноприйнятих інструментів кількісної оцінки "небезпечності" конкретної технічної уразливості є CVSS (Common Vulnerability Scoring System). CVSS надає бальну шкалу від 0.0 до 10.0, де 10 означає максимально критичну уразливість (Табл 2.4). Базова група метрик CVSS включає фактори експлуатованості (як легко використати: чи потрібні привілеї, чи потрібна взаємодія користувача, чи можлива віддалена атака тощо) та впливу (який вплив на конфіденційність, цілісність, доступність у разі експлуатації). Наприклад, уразливість, яка дозволяє будь-якому мережевому користувачу повністю захопити систему (повний компрометуючий вплив на C, I, A) – отримає в CVSS бал ~10 (критичний). Натомість локальна уразливість, яка потребує входу під обліковим записом і лише незначно впливає на роботу – може мати CVSS-бал ~4 (середній). CVSS широко використовується у звітах сканерів та пентестів, щоб пріоритезувати виправлення: зазвичай CVSS ≥ 7.0 вважається високим ризиком, який слід виправити негайно. Однак варто зазначити, що CVSS-бал – це усереднена абстрактна оцінка. Вона не враховує контекст конкретної організації.

Наприклад, уразливість з CVSS 9.0 у програмі, яка не використовується в бойовому режимі в даній мережі, на практиці може не становити великого ризику. Для цього CVSS має темпоральні та середовищні метрики: можна знижувати оцінку,

якщо вже існує патч чи експлойт недоступний; або підвищувати, якщо вразливий хост – критичний сервер (цю можливість дають Environmental Score). У підсумку, CVSS корисна як стандартна мова спілкування між ІБ-фахівцями: забезпечує об'єктивність у тому сенсі, що дві різні команди, незалежно оцінивши уразливість за CVSS, отримають однаковий результат, що сприяє узгодженості дій.

Таблиця 2.4

Система бальної оцінки вразливостей CVSS

Базовий бал	**Рівень**	**Опис**
0.0	None(Відсутній)	Вразливість відсутня або недосяжна.
0.1 – 3.9	Low(Низький)	Вплив мінімальний, експлуатація складна.
4.0 – 6.9	Medium(Середній)	Можливий компроміс, але вимагає умов
7.0 – 8.9	High(Високий)	Значний вплив на конфіденційність/цілісність, часто віддалений доступ.
9.0 – 10.0	Critical(Критичний)	Повний контроль над системою, віддалене виконання коду, відсутність взаємодії з користувачем.

Модель FAIR (Табл. 2.5.) - кількісний аналіз ризику. Для стратегічного рівня управління ризиками (особливо фінансовими) розроблено модель FAIR (Factor Analysis of Information Risk). Вона намагається перекласти кіберризики в грошовий вимір і надати чітку методику оцінки ймовірності і впливу. В основі FAIR - два ключових показники: Loss Event Frequency (частота події втрати) та Loss Magnitude (величина втрати). Loss Event Frequency ділиться на: Threat Event Frequency (як часто

потенційний зловмисник спробує атакувати конкретний об’єкт) та Vulnerability (ймовірність того, що спроба буде успішною, тобто вразливість спрацює).

Таблиця 2.5

Інтегрована Матриця оцінки впливу та ймовірності

Ймовірність / Вплив	**Незначний (Low Impact) (CVSS < 4.0)**	**Помірний (Medium Impact) (CVSS 4.0–6.9)**	**Значний (High Impact) (CVSS 7.0–8.9)**	**Критичний (Critical Impact) (CVSS 9.0–10.0)**
Майже напевно (>90% / щомісяця)	Середній (M)	Високий (H)	Екстремальний (E)	Екстремальний (E)
Ймовірно (50-90% / щороку)	Низький (L)	Середній (M)	Високий (H)	Екстремальний (E)
Можливо (20-50% / раз на 3 роки)	Низький (L)	Середній (M)	Високий (H)	Високий (H)
Малоймовірно (<20% / раз на 10 років)	Низький (L)	Низький (L)	Середній (M)	Середній (M)

Loss Magnitude теж ділиться на: Primary Loss (прямі втрати - наприклад, час простою, витрати на відновлення) та Secondary Loss (непрямі - штрафи регуляторів, шкода репутації, відтік клієнтів). На практиці оцінка за FAIR вимагає збору даних: статистики інцидентів, фінансових показників, експертних оцінок [18].

На відміну від якісних матриць, FAIR вимагає більше зусиль, але забезпечує набагато більш предметну розмову з керівництвом, оскільки представити ризик у вигляді “$X млн потенційних збитків на рік” – зрозуміліше, ніж “високий ризик”. Як зазначає CIS (Center for Internet Security), FAIR переводить суб’єктивні категорії в долари і центи, надаючи єдину мову для IT і бізнесу. Великі компанії та банки все частіше впроваджують FAIR або її похідні для прийняття рішень щодо кіберстрахування, розподілу бюджету на безпеку, обґрунтування витрат на SOC тощо.

Байєсові моделі та інші підходи. В академічних колах і деяких високонадійних системах (наприклад, авіація, АСУ ТП) застосовуються байєсові мережі та статистичні моделі для оцінки кіберризиків. Байєсові мережі дозволяють створити граф залежностей між різними подіями та умовами (вузлами мережі) і обчислити ймовірності цільової події з урахуванням цих залежностей.

Наприклад, можна змоделювати вузли: “наявна непатчена уразливість”, “активний експлойт у дикому середовищі”, “успіх експлуатації”, “спрацювання детектора” тощо – з заданими ймовірностями, і розрахувати загальну ймовірність успішної атаки. При оновленні даних (наприклад, виходить патч, змінюється один із параметрів) – мережа перераховує ризик. Байєсовий підхід корисний, коли є статистичні дані або експертні оцінки про ймовірності часткових подій. У реальності ж такі дані отримати важко, тому часто замість суворої математики використовують простіші інструменти.

NIST RMF та інші фреймворки. Управління ризиками кібербезпеки у критичній інфраструктурі часто регламентується національними чи галузевими стандартами. NIST Risk Management Framework (RMF) – підхід, який поєднує класифікацію систем за рівнями впливу (високий, середній, низький по критеріях CIA), вибір відповідних контролів (на основі NIST 800-53), оцінку ефективності впроваджених контролів і авторизацію системи до експлуатації з урахуванням резидуальних ризиків.

В Україні впроваджується система стандартів, сумісних з ISO 2700x та NIST, але адаптованих до національних реалій. Держспецзв’язку, відповідальна за захист державних інформаційних ресурсів, випустила низку нормативних документів з

оцінки захищеності, які фактично виконують функцію ризик-менеджменту: аналіз загроз, визначення можливих каналів реалізації, розрахунок ризиків (часто таки ж матричним способом, що підтверджується методиками оцінки стану кібербезпеки).

Прикладом національної методики є Методика оцінки ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури (розробка НДІ інформаційної безпеки), яка пропонує перемножувати бальну оцінку ймовірності загрози на бальну оцінку наслідків для визначення інтегрального ризику. Цей підхід подібний до матриць, розглянутих вище, і є інтуїтивним для інженерів. Разом з тим, у секторах з підвищеною небезпекою (наприклад, ядерна енергетика) можуть застосовуватися складніші сценарні аналізи: моделювання розвитку атаки і її фізичних наслідків, оцінка ризиків у термінах перерваної генерації енергії, можливого техногенного збитку тощо.

Ризики для конфіденційності, цілісності, доступності. При оцінці впливу кіберінцидентів зазвичай розглядаються три класичні виміри: конфіденційність (втрата контролю над чутливою інформацією), цілісність (несанкціонована зміна або знищення даних) та доступність (недоступність сервісів, відмова в обслуговуванні).

Для критичної інфраструктури часто найбільшу вагу має доступність, адже припинення роботи енергомережі чи транспорту одразу веде до відчутних наслідків. Однак і про конфіденційність не можна забувати: витік даних про технологічні процеси чи персонал може полегшити противнику підготовку атак. Вплив зазвичай оцінюється з позиції "найгіршого ефекту на одну з цих трьох сфер". Додатково враховуються фінансові наслідки (прямі збитки, штрафи) та репутаційні (втрата довіри, негативний розголос). Наприклад, якщо внаслідок атаки відбудеться масштабний блекаут, компанія зазнає не тільки фінансових втрат від простою, а й можливих судових позовів, урядового розслідування, зниження акцій тощо – усе це треба намагатися оцінити або принаймні описати якісно [19].

У США, прикладом моделі для критичної інфраструктури діє підхід "випробування на стресостійкість" для енергосектору: компанії мають моделювати сценарії (в т.ч. кібер) з екстремальними наслідками і звітувати про здатність до них відновитися. В Європейському Союзі (ENISA) запроваджуються мережеві коди

кібербезпеки для енергетики, які вимагають від операторів проводити регулярну оцінку ризиків і впроваджувати заходи згідно з принципом пропорційності ризику. Стандарти IEC 62443 для промислових систем також містять розділи про оцінювання ризиків і визначення рівнів безпеки (Security Levels) для компонентів. Національні регулятори (як от НКРЕКП в Україні для енергетики, НБУ для банків) видають галузеві вимоги до кібербезпеки, фактично засновані на ризик-орієнтованому підході: наприклад, НБУ зобов'язує банки розраховувати показники ризику інформбезпеки і подавати їм у складі регулярної звітності.

Отже, оцінка впливу та імовірності кіберінцидентів може бути виконана на різних рівнях точності – від кольорових матриць до фінансових моделей. Важливо, що кінцева мета всіх цих підходів одна: правильно пріоритезувати ресурси на захист. Ризики, які визнані неприйнятними (наприклад, критичні в червоній зоні матриці або з потенційною шкодою у десятки мільйонів доларів), мають бути або знижені (впровадити додаткові засоби захисту), або передані (страхування, контрактне перенесення), або прийняті під відповідальність керівництва. Практика показує, що у критичній інфраструктурі більшість значних ризиків намагаються знизити – через високу ставку наслідків для суспільства.

2.5. Зведення результатів аналізу та вимоги до інструментарію

Проведений аналіз засвідчив, що кожен домен критичної інфраструктури стикається зі специфічним набором загроз, проте багато із цих загроз мають спільні риси і високий потенціал перехресного впливу. Наприклад, атаки типу DDoS становлять ризик для будь-яких публічних сервісів – чи то банківського вебпорталу, чи сайту енергокомпанії, чи державного реєстру. Цільові атаки APT з використанням складних багатоетапних кампаній (фішинг – бекдор – рух всередині мережі – саботаж) однаково небезпечні для енергетики, зв'язку, держсектору, хоча конкретні техніки (набори експлойтів, шкідливих програм) можуть відрізнятися. Це підтвердилося у кіберінцидентах 2022–2023 рр.: ті самі групи зловмисників (наприклад, Sandworm, APT28) здійснювали операції одночасно проти енергетичних

компаній, телеком операторів і держустанов. Отже, підхід до захисту має бути комплексним і скоординованим. Класифікація загроз надала фундамент для розуміння, які типи атак найбільш характерні та небезпечні в кожному секторі.

Наприклад, для умовної енергокомпанії найвищий ризик – деструктивна атака на OT-системи, яка може призвести до катастрофічного збою енергопостачання. Ймовірність такої атаки у воєнний час висока, як показали випадки з Industroyer2. В фінансовому секторі критичним ризиком може бути масштабний витік або знищення даних клієнтів (удар по цілісності та конфіденційності), що загрожує як фінансовими втратами, так і втратою довіри. В урядовому секторі – порушення надання державних послуг через комбіновані DDoS і атаки на дані (наприклад, виведення з ладу порталу держпослуг під час кризи).

Вимоги до засобів управління кіберризиками. На основі виявлених загроз і їх оцінки можна сформулювати вимоги до інструментів, які мають бути задіяні для ефективного управління кіберінцидентами у кризових ситуаціях. Під управлінням мається на увазі увесь цикл: виявлення – реагування – відновлення – попередження повторення. У кризових умовах (воєнний час, масовані атаки) особливо важливими стають автоматизація та швидкодія. Тому сучасний набір інструментів включає:

Платформи SIEM (Security Information and Event Management): для централізованого збору даних, їх кореляції та своєчасного оповіщення про інциденти. Вимоги: здатність обробляти великий обсяг логів у режимі реального часу, гнучкі правила кореляції (в т.ч. поведінковий аналіз), інтеграція з Threat Intelligence (отримання актуальних IOC). SIEM має забезпечувати стійкість у кризових умовах – тобто мати резервування і захист власної бази (щоб атакуючий не міг її підробити або видалити журнали).

Платформи SOAR Security Orchestration, Automation and Response для автоматизації і оркестрації реакції на інциденти у кризовій ситуації, коли кількість інцидентів може бути велика, SOAR може виконувати рутинні дії без участі людини: ізолювати скомпрометовані хости, блокувати IoC на фаєрволах, створювати тікети відповідальним тощо. Вимоги до SOAR: гнучкі playbooks (сценарії реакцій) для різних типів атак, інтеграція з існуючими засобами (SIEM, системами управління

мережами, Active Directory, засобами резервування даних), можливість роботи в режимі обмеженого інтернет-зв'язку (на випадок, якщо зовнішні канали порушені атакою).

Платформи Threat Intelligence (TI), у кризовій ситуації допомагають оперативно отримувати й застосовувати розвіддані про нові загрози. Наприклад, при надходженні свіжих IOC щодо ворожого шпигунського ПЗ – автоматично завантажувати ці IOC до SIEM та систем захисту кінцевих точок. Вимоги: підтримка стандартів обміну (STIX/TAXII), наявність механізмів пріоритезації (щоб у потоці TI виділяти найрелевантніші для своєї галузі), інтеграція з SOC-процесами (аналітики мають легко збагачувати інциденти даними TI).

Засоби моніторингу мереж і виявлення аномалій, а саме IDS/IPS, а також рішення, основані на машинному навчанні (UEBA, NDR – Network Detection and Response) в умовах, коли атаки можуть використовувати невідомі раніше методи (0-day, власні малвари), сигнатурних методів може бути недостатньо. Вимоги: наявність аномалійного виявлення – інструменти мають профілювати нормальну роботу систем та виявляти відхилення (наприклад, раптове підвищення трафіку на нехарактерні порти, нетипова активність облікового запису). Такі системи повинні вміти працювати у вкрай зашумленому середовищі (під час атаки багато аномалій – потрібна фільтрація) та видавати мало хибних спрацьовувань.

Системи резервного копіювання та відновлення в контексті кризового управління кіберінцидентами інструменти резервування (backup) стають критично важливими – особливо для загроз типу ransomware чи вайперів. Вимоги до них: ізольованість (щоб шкідливе ПЗ не змогло знищити резервні копії), регулярність (автоматичне створення копій ключових даних) та перевіреність відновлення (план DRP має тестуватися). Наприклад, використання immutable backups – резервних копій, що не можуть бути змінені після створення – суттєво підвищує життєстійкість даних [20].

Спеціалізовані засоби для OT-безпеки для об'єктів на кшталт енергомереж чи заводів потрібні для моніторингу промислових протоколів (SCADA-IDS), контролери безпеки PLC, мережеві екрани з розумінням OT-трафіку. Вимоги: сумісність з

промисловими стандартами (MODBUS, DNP3, IEC 60870-5-104 тощо), пасивне прослуховування без впливу на процес (щоб не спричиняти збоїв), здатність працювати в режимі ізоляції (якщо підприємство відключене від інтернету, локальні SOC-інструменти повинні продовжувати функціонувати автономно).

Інструменти керування вразливостями та конфігураціями потрібні щоб зменшити ймовірність успішних атак, необхідні засоби постійного сканування і аудиту. Вимогами є централізований огляд стану всіх систем, автоматичне зіставлення з базами патчів (і пріоритизація патч-менеджменту відповідно до ризику), інтеграція з workflow (створення завдань на виправлення для IT-відділу). Це дозволить у фоновому режимі підтримувати "гігієну" інфраструктури, знижуючи ризик компрометації під час кризи.

Кризовий кіберінцидент потребує злагоджених дій багатьох команд (IT, безпека, управління, зв'язки з громадськістю). Корисними є інструменти типу Crisis Management System або принаймні захищені канали зв'язку (месенджери, відеоконференції) для координації. Вимоги: висока надійність і захищеність (можливо, використання out-of-band комунікацій, якщо корпоративна мережа скомпрометована), журналювання дій (щоб пост-фактум проаналізувати, які рішення приймалися і коли).

Ключовими функціями, які мають покриватися інструментарієм мають бути:

- Моніторинг в реальному часі усіх критичних вузлів (мереж, серверів, контролерів) із застосуванням інтелектуальних алгоритмів виявлення.
- Автоматичне реагування на типові інциденти за наперед визначеними сценаріями (ізоляція, блокування, повідомлення відповідальних осіб).
- Можливість глибокого аналізу причин інциденту, збору доказів (журнали, пам'ять, образи дисків) – це потребує наявності як програмних інструментів (форензик-комплекти), так і процедур.
- Оркестрація та централізація усіх компонентів (SIEM, SOAR, TI, сканери) повинні працювати узгоджено, дані – зводитись в єдиний "панель" для SOC. Це спрощує управління під час стресу, коли часу розбиратися по окремих системах немає.

- Розгортання резервних серверів логування, ізольовані консолі моніторингу, двофакторна автентифікація для адміністраторів SOC.

Умовно кажучи, інструментарій управління кіберінцидентами у критичній інфраструктурі можна порівняти з “нервовою системою” організації, яка чутливо реагує на подразники (атаки) і миттєво ініціює рефлекси-відповіді. Від її спроможності залежить, чи переросте інцидент у кризу, чи буде локалізований і знешкоджений з мінімальними втратами.

Багато світових постачальників пропонують комплексні рішення, які включають згадані компоненти. Наприклад, платформа Microsoft Sentinel позиціонується як cloud-SIEM з елементами SOAR, тісно інтегрований з TI від Microsoft та засобами захисту кінцевих точок (Defender). Інше рішення – IBM QRadar + Resilient – зв’язка SIEM та SOAR, що дозволяє від реагування в один клік переходити до запуску планів реагування Resilient. Для критичного підприємства важливо обирати такі рішення з урахуванням національних особливостей.

ВИСНОВКИ ДО РОЗДІЛУ 2

У другому розділі було проведено комплексне дослідження ландшафту кіберзагроз для критичної інфраструктури та методів їхнього виявлення й аналізу. Були класифіковані основні типи загроз за галузевими доменами (енергетика, транспорт, зв’язок, фінанси, охорона здоров’я, водні ресурси, держуправління) із конкретними прикладами атак 2022–2024 рр., пов’язаних значною мірою з військовою агресією (DDoS-кампанії, деструктивні malware, атаки на ланцюги постачання тощо). Розглянуто сучасні інструменти виявлення вразливостей – від традиційних (сканери, пентест) до інтелектуальних систем моніторингу (SIEM, IDS, SOC-платформи) – та їх роль у запобіганні інцидентам. Показано, що ефективне виявлення вразливостей регламентується міжнародними стандартами (ISO 27005, NIST SP 800-30) і має спиратися на кращі практики (безперервний процес, пріоритезація за ризиком).

Далі, були висвітлені методи аналізу загроз: модель STRIDE дала систематизацію потенційних загроз, DREAD – інструмент оцінки їх критичності, PASTA – глибокий ризик-орієнтований процес моделювання атак, MITRE ATT&CK – сучасний довідник технік нападників, Kill Chain – концепція життєвого циклу кібератаки. На основі цього арсеналу організація може будувати проактивний захист, орієнтований на зрив ланцюгів атаки і раннє виявлення. Відзначено тренди – застосування AI для детектування загроз і посилення кіберрозвідки – що будуть розвиватися і надалі.

Була продемонстрована методика оцінки кіберризиків: якісні (матриці) і кількісні (CVSS, FAIR) підходи. Особливий акцент зроблено на важливості врахування впливу на критичні триади CIA та фінансово-репутаційних наслідків. Наведено приклад ризик-матриці для енергокомпанії та показано, як на практиці визначаються зони неприйнятного ризику. Розглянуто моделі ризик-менеджменту, застосовні до критичної інфраструктури (NIST RMF, національні методики ДССЗЗІ), що формують основу політик безпеки.

РОЗДІЛ 3
ІСНУЮЧІ МЕТОДИ ТА МОДЕЛІ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ У КРИЗОВИХ УМОВАХ

3.1. Операційні структури SOC, CSIRT, IRT

Операційні центри безпеки SOC, команди реагування на комп'ютерні інциденти (Computer Security Incident Response Team, CSIRT/CIRT) та команди реагування на інциденти (Incident Response Team, IRT) становлять різні рівні організаційної структури в системі кіберзахисту. SOC – це центральний функціональний підрозділ організації, який цілодобово моніторить усю IT-інфраструктуру, аналізує події безпеки і виконує початкове реагування на загрози в режимі реального часу. Зокрема, SOC координує роботу SIEM-систем, збирає логи з мережевих пристроїв, серверів і кінцевих точок, проводить кореляцію подій та ініціює перші кроки реагування. CSIRT – це спеціалізована команда, яка управляє повним життєвим циклом інциденту: від виявлення і аналізу до локалізації, ліквідації наслідків та відновлення нормального функціонування. CSIRT зазвичай включає фахівців різних профілів (аналітиків, інженерів, менеджерів, юристів), їхньою метою є мінімізувати шкоду від інцидентів і забезпечити безперервність критичних сервісів [10].

Наявність CSIRT визначена у стандартах і рекомендаціях з інформаційної безпеки (зокрема NIST SP 800-61), де така команда окреслена як група, що допомагає відповідати на комп'ютерні інциденти в організації.

Термін CERT (Computer Emergency Response Team) часто використовується як синонім CSIRT, особливо на національному або галузевому рівні. IRT (Incident Response Team) у сучасній практиці здебільшого означає внутрішню команду реагування на інциденти у великих організаціях і має ті самі цілі – швидке виявлення, локалізацію, розслідування та усунення кіберзагроз. Так, у широкому розумінні IRT – це міждисциплінарна група, що складається зі спеціалістів IT, безпеки, юридичних

відділів і керівництва, яка оперативно реагує на порушення і відновлює нормальну роботу систем.

У багаторівневій системі кіберзахисту SOC**,** CSIRT/CERT **і** IRT виконують доповнювальні ролі. SOC зазвичай функціонує на рівні самої організації, забезпечуючи безперервне моніторингове спостереження та своєчасну обробку подій безпеки. CSIRT (чи CERT-UA в контексті України) часто виступає центральним координаційним органом, який веде глобальний аналіз загроз та взаємодіє з іншими організаціями і державними структурами [14].

Наприклад, за законодавством України Державний центр кіберзахисту (CERT-UA) виконує роль національного CSIRT та одночасно діє як централізований SOC для всіх учасників кіберекосистеми країни. Це означає, що після виявлення інциденту локальним SOC він може скерувати інформацію до CSIRT/CERT для подальшої деталізації та координації на ширшому рівні.

З іншого боку, під час великих криз (військові дії, масштабні атаки) на порядку денному постає питання про швидке обміну інформацією між державними і галузевими центрами. На міжнародному рівні існують кооперації між CERT-UA та аналогічними структурами інших країн (наприклад, кооперація ENISA з CERT-EU) або зі Сполученими Штатами (US-CERT/CISA). Таке співробітництво дозволяє оперативно розповсюджувати інформацію про нові загрози, вразливості та атаку на критичну інфраструктуру.

Типова архітектура SOC передбачає складну інфраструктуру з датчиків та колекторів подій (з SIEM-системою), аналітичні робочі місця для інцидент-аналитиків, а також інструменти захисту на кінцевих точках і мережі (EDR, IDS/IPS). У SOC звичайно діє процедура обробки інцидентів за логікою «4С» (знайти, класифікувати, локалізувати, ліквідувати) або відповідно до рекомендацій NIST – з етапами підготовки, виявлення/аналізу, локалізації, ліквідації, відновлення та уроків. Моделі координації між структурами можуть бути горизонтальними (горизонтальні обміни інформацією між SOC компаній того ж сектору чи галузі) або вертикальними (подача звітів від SOC, потім CSIRT, далі міжнародні CERT). В умовах кризи (зокрема

війни або масованої кібератаки) ефективність цих структур ускладнюється обмеженими ресурсами і підвищеним навантаженням.

Наприклад, в умовах гібридної війни проти України відзначено стрімке зростання кібератак (зокрема рансомваре), а оператори критичної інфраструктури стикаються з труднощами у своєчасному виявленні та реагуванні на них. При цьому зростання обсягу інцидентів зазвичай супроводжується браком кваліфікованих аналітиків і необхідністю приймати рішення в умовах обмеженої інформації та тиску часу. У таких ситуаціях важливими стають оперативна координація з урядовими центрами (наприклад, з CERT-UA) і використання загальних засобів обміну даними (платформи MISP, Національний центр сповіщення про кібератаки тощо) [4].

3.2. Інструменти моніторингу та виявлення SIEM, EDR, NDR, IDS/IPS, SCADA/ICS моніторинг

Сучасний SOC використовує низку спеціалізованих інструментів для моніторингу й аналізу безпеки. **SIEM** (Security Information and Event Management) – це система збору та кореляції журналів подій з різноманітних джерел (мережевих пристроїв, серверів, додатків, інколи і SCADA-контролерів) з метою виявлення аномалій чи відомих загроз. Наприклад, IBM QRadar – це SIEM-платформа, яка збирає логи з мережевих пристроїв, серверів та кінцевих точок, виконує нормалізацію і кореляцію даних та присвоює пріоритет сповіщенням на основі ризику.

Подібно, Splunk Enterprise Security аналізує великі обсяги машинних даних у реальному часі й забезпечує візуалізацію KPI та інструменти для розслідування інцидентів. SIEM-системи часто діють як «мозок» SOC, надаючи централізовану панель для аналітиків і підтримуючи інтеграцію з іншими засобами (наприклад, завдяки додатковим модулем XDR для отримання поглибленої телеметрії).

EDR (Endpoint Detection and Response) – рішення, що встановлюються на кінцеві пристрої (сервери, ПК, мобільні гаджети) і забезпечують моніторинг поведінки та захист на самих точках. EDR системи виявляють підозрілу активність на хостах, виконують аналіз файлів і процесів у реальному часі, а також забезпечують

засоби віддаленого реагування (ізоляція, видалення шкідливого коду). Навпаки, NDR (Network Detection and Response) спирається на аналіз мережевого трафіку – він фіксує трафік, застосовує сигнатури та машинне навчання для виявлення атак на мережевому рівні.

Обидва підходи взаємодоповнюючі: як зазначає аналітика, NDR фокусується на виявленні аномалій у трафіку, пропонуючи широкий огляд мережі, тоді як EDR детальніше досліджує активність на окремих кінцевих пристроях. За потреби вони можуть працювати разом у складі XDR-платформи або окремо: наприклад, CrowdStrike Falcon і Microsoft Defender – популярні EDR-рішення, а Zeek (колишній Bro) та Suricata – відомі системи мережевого моніторингу/IDS з відкритим кодом. IDS/IPS (Intrusion Detection/Prevention System) – це традиційні рішення, що слідкують за мережевим трафіком або активністю на хості та генерують сповіщення при виявленні відомих підписів загроз [8].

IDS пасивно повідомляє про загрозу (трафік при цьому продовжує надходити), тоді як IPS може діяти «on-path» і блокувати підозрілий трафік (тобто припиняти потік). У комплексі SOC-аналітики часто поєднують інструменти IDS/IPS з системою SIEM: перші відправляють сигнали до SIEM, де вони корелюються з іншими подіями, а потім відповідні процедури реагування запускаються автоматично чи вручну.

Для критичних галузей (енергетика, транспорт, телеком) важливо застосовувати інтегровані рішення, що враховують особливості промислових мереж і SCADA/ICS-систем. Системи SCADA/ICS керують фізичними процесами на об’єктах критичної інфраструктури (електростанції, водопостачання тощо) і зазвичай використовують спеціалізовані протоколи (Modbus, DNP3 тощо). Даня системи часто функціонують у режимі реального часу та не можуть просто перезавантажуватись без зупинки виробництва. Тому для їхнього захисту розроблені спеціалізовані методи виявлення: наприклад, аналіз нетипових команд до ПЛК, моніторинг відповідних SCADA-протоколів, використання honeynet для виявлення вторгнень.

Комерційні рішення на кшталт Splunk ES або QRadar мають модулі для збору даних з промислових систем, а також можуть обробляти просторові і часові аномалії в поведінці сенсорів. У відкритому просторі прикладами є Zabbix (система

моніторингу, яку можна налаштувати на опитування пристроїв OT), OpenVAS (сканер вразливостей, застосовний до IP-мереж) та Zeek/Suricata (для аналізу трафіку OT).

Застосування подібних інструментів підвищує ситуаційну обізнаність під час кризи: об'єднуючи дані з IT- і OT-мереж, SOC/CSIRT може швидко бачити хід подій, зіставляти інформацію з різних джерел і приймати рішення з урахуванням загального стану критичних систем (наприклад, виведення під контролем або аварійне зупинення обладнання у відповідь на хакерську атаку).

3.3. Моделі прийняття рішень у кризових ситуаціях OODA, PDCA

Існують різні фреймворки оперативного прийняття рішень, що адаптовані до умов кібербезпеки. Одна з найвідоміших – цикл OODA (Observe–Orient–Decide–Act), запропонований полковником США Джоном Бойдом для військових цілей. У кібербезпеці OODA застосовується як ітеративна модель ухвалення рішень під час атаки: фаза Observe відповідає за виявлення загроз і збір даних (моніторинг мережі, логів, телеметрії); Orient – аналіз і тлумачення цих даних з урахуванням попереднього досвіду і контексту, визначення масштабу і характеру інциденту; Decide – розробка плану реагування (визначення заходів утримання та ліквідації); Act – безпосереднє виконання обраних заходів (ізоляція систем, видалення шкідливих програм, відновлення за допомогою резервних копій).

Ключова властивість OODA – швидка, гнучка перебудова пріоритетів у відповідь на зміну ситуації. Як зазначають фахівці, скорочений цикл OODA дає змогу «випереджувати» противника: поки він орієнтується у нових обставинах, оборонці вже діють і змінюють умови бою на свою користь. Для SOC ця модель означає, що крім фази «спостереження» (моніторингу і аналітики), вирішальним є «діяти» – тобто ефективно проводити заходи реагування [9].

У концепції SOC високого рівня поєднання ситуаційної обізнаності (Observe/Orient) з «вирішальними діями» (Decide/Act) характеризує його

результативність. Така модель добре підходить для умов високої невизначеності й швидкоплинних атак, коли рішення треба приймати швидко без повного аналізу.

PDCA (Plan–Do–Check–Act) – інша широко відома ітеративна модель, що походить із теорії управління якістю Демінга. У кібербезпеці її використовують для безперервного вдосконалення процесів інцидент-менеджменту. Фаза Plan включає планування політик і процедур реагування; Do – практичне впровадження заходів (тренування персоналу, тестування сценаріїв); Check – перевірку ефективності (аналіз звітів, навчання за «пост-інцидентними» оглядами); Act – внесення коректив (оновлення планів, оптимізація інструментів).

Циклічність PDCA забезпечує поступове підвищення готовності до інцидентів – наприклад, згідно зі стандартом ISO/IEC 27035, керування інцидентами організовується в кілька фаз (планування, виявлення, оцінка, реагування, уроки), що повторюються. PDCA дає чітку структуру і стимулює збирання даних для аналізу, але його «планово-перевірочний» підхід часто вважають занадто повільним для екстремальних випадків.

Практика показує, що OODA і PDCA взаємодоповнюють одна одну. Поки OODA забезпечує оперативну реакцію на інцидент, PDCA – це більш глобальний цикл вдосконалення, який забезпечує підготовку і «розбори польотів». Наприклад, фази виявлення і аналізу можуть розглядатися як Observe–Orient у OODA та як «Check» у PDCA (перевірка результативності останніх дій), а фаза «Lessons Learned» зазвичай замикає PDCA і підсилює наступне коло OODA. Експерти відзначають, що PDCA сприяє збиранню уроків та удосконаленню процедур загалом, тоді як OODA фокусує увагу на швидкості і гнучкості реакції.

Таким чином, в практиці SOC або кризової команди часто застосовують змішаний підхід: базують процеси на PDCA-моделі (для підготовки, документування політик, регулярних вправ), але у реальних інцидентах орієнтуються на ритмічність OODA-циклу, щоб скоротити час виявлення і реагування. У порівнянні, OODA зазвичай демонструє перевагу у швидкості й адаптивності, а PDCA забезпечує ретельність і контроль якості реакції.

3.4. Підходи до автоматизації реагування на кіберінциденти у SOAR

SOAR (Security Orchestration, Automation and Response) – це концепція та класи інструментів, які інтегрують різні системи безпеки (SIEM, EDR, антивірусні рішення, мережеві сенсори тощо) в єдиний автоматизований конвеєр реагування. Платформи SOAR надають можливість формалізувати типові сценарії реагування (playbooks) у вигляді визначених робочих процесів. Коли виявлено підозрілий інцидент, SOAR-система може автоматично зібрати потрібний контекст (запити до SIEM, виклик скриптів для перевірки), ізолювати уражені об’єкти та навіть розсилати сповіщення за заздалегідь прописаними правилами. При цьому аналітик може втручатися в будь-якому місці сценарію для уточнення дій [12].

Архітектура SOAR-платформи зазвичай включає конектори до сторонніх систем (logstore, threat intelligence, ticketing), движок оркестрації (який запускає playbook’и) та інтерфейс користувача. Наприклад, SOAR-інструменти Cortex XSOAR (Palo Alto Networks), IBM Resilient або Splunk Phantom підтримують інтеграцію з популярними SIEM і EDR-рішеннями і постачають бібліотеки стандартних playbook’ів (наприклад, «реакція на фішинг», «ліквідація підозрілих процесів»). Як описує Elastic, SOAR «координує й автоматизує ключові процеси на єдиній платформі», тісно поєднуючись із SIEM для приведення до дії знайдених загроз. Тобто SIEM відповідає за виявлення і оповіщення, а SOAR – за виконання наступних кроків: автоматизоване блокування чи розслідування.

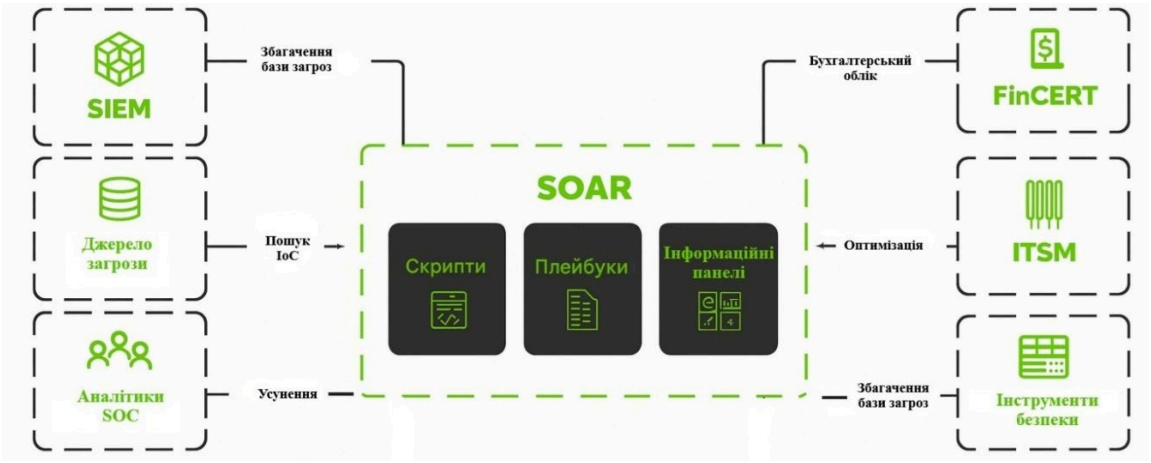

Рис. 3.1. Модель конвеєру реагування на кіберзагрози SOAR

У кризових умовах автоматизація має особливо великий ефект. Використання SOAR значно зменшує час реакції (адже повторювані дії виконуються без участі людини) і рівень помилок через «людський фактор». Наприклад, SOAR може миттєво (без затримок на ручне введення) ізолювати в мережі пристрій, позбавити його доступу чи розгорнути скрипти ліквідації – усе за декілька секунд. Крім того, автоматизовані плейбуки гарантують однорідність обробки типових інцидентів та полегшують навчання нових аналітиків. Розробка і впровадження SOAR-підходів у критичних секторах дозволяє, зокрема, скоротити середній час реагування (MTTR), підтримувати єдиний комунікаційний процес і акцентувати увагу команди на найскладніших аспектах розслідування [13].

3.5. Метрики ефективності реагування, показники ресурсного розподілу

- Оцінка результативності процесу реагування передбачає низку метрик і KPI/KRI. Основні технічні метрики включають:
- MTTD (Mean Time to Detect) – середній час від початку інциденту до моменту його виявлення.
- MTTI (Mean Time to Identify) – час від спрацювання системи моніторингу до остаточного ідентифікування природи інциденту (наприклад, назв зловмисного ПО).
- MTTR (Mean Time to Respond/Recover) – середній час від виявлення до усунення інциденту та відновлення нормальної роботи.
- Incident Containment Time – час від виявлення інциденту до локалізації та припинення поширення шкоди.

Класичним KPI для SOC/CSIRT є MTTD та MTTR, які регулятори й аудитори вимагають для оцінки оперативності реагування. Крім того, до аналітики часто входять частота інцидентів, їхня середня тяжкість (середня очікувана вартість або втрати), відсоток неправдивих спрацювань (False Positives) тощо. Типовими KPI можуть бути також обсяг моніторингу (кількість оброблених пристроїв/логів), кількість відкритих і закритих кейсів, рівень дотримання SLA на інцидент тощо. KRI

(Key Risk Indicators) для SOC/CSIRT можуть включати, наприклад, частку невиправлених вразливостей у критичних системах, кількість днів, протягом яких не було резервних копій, або щорічні витрати на кібервтручання у порівнянні з запланованим бюджетом [3].

Щодо ресурсних показників, оцінюють витрати часу на реагування (кількість людино-годин), прямі фінансові витрати на усунення інциденту та відновлення, а також навантаження персоналу (навантаження чергових, відсоток часу аналітиків, відпрацьованого на інциденти). Наприклад, аналітичні панелі SOC зазвичай відображають фактичне навантаження на кожен з інструментів (скільки інцидентів оброблено, скільки – в черзі) та статус пріоритизації. Деякі компанії вказують кількість сертифікованих аналітиків у команді і витрачені на навчання години як KPI розвитку. Усі ці показники слугують для звітності і прийняття рішень з розподілу ресурсів у кризу.

Важливу роль відіграє інструментарій дашбордів. Графічні панелі моніторингу ситуації в реальному часі дозволяють бачити ключові метрики (MTTD/MTTR, кількість нових інцидентів, категорії інцидентів за пріоритетом) та аналізувати тренди. Ускладнюють розрахунок ефективності фрагментарність даних (дані можуть бути розсіяні по кількох системах SIEM, EDR, сервісах зовнішніх постачальників) і необхідність узгодження форматів. Тому в кризовому управлінні прагнуть до централізації звітності – наприклад, за стандартами NIST чи ENISA рекомендується використовувати єдині схеми класифікації інцидентів і уніфіковані формати звітності, щоб показники можна було порівнювати у масштабі всієї інфраструктури чи сектору [21].

3.6. Порівняльна оцінка існуючих методів та ідентифікація недоліків

Розглянуті методи реагування можна узагальнити як три взаємодоповнюючі напрями: організаційні (SOC, CSIRT/IRT), технологічні (SIEM, EDR, NDR, SOAR тощо) та аналітичні/процедурні (моделі прийняття рішень, підходи до автоматизації, метрики). Порівняльний аналіз показує, що SOC і CSIRT забезпечують різні рівні

огляду: SOC швидко виявляє та ініціює первинний захист на рівні організації, а CSIRT координує більший фронт реагування (включно з міжсекторним чи міжнародним співробітництвом). SOAR та SIEM суттєво прискорюють детекцію і відповідь за рахунок автоматизації: наприклад, SOAR значно знижує час виконання операцій реагування, тоді як SIEM як централізована система журналів прискорює виявлення аномалій.

Загалом, автоматизовані рішення є найшвидшими у маршрутизації сповіщень і виконанні реактивних дій, але потребують наперед налаштованих сценаріїв і якісних даних. Моделі OODA та PDCA відрізняються підходом: OODA вимагає високої адаптивності та швидкості при одночасних обмежених деталях, тоді як PDCA краще забезпечує комплексне покриття за рахунок детального планування і аналізу. З цієї точки зору, найкращий результат дає поєднання: швидке прийняття рішень (OODA) у поєднанні з постійним вдосконаленням (PDCA).

Однак існуючі моделі мають низку недоліків:

По-перше, обмеженість людських ресурсів**:** у багатьох компаніях SOC/CSIRT працює в умовах дефіциту фахівців і підвищеного стресу, особливо в кризу, коли кількість інцидентів різко зростає.

По-друге, фрагментарність даних**:** різні інструменти часто зберігають інформацію у власних сховищах, що ускладнює її кореляцію і загальний огляд. Це призводить до «сліпих зон» спостереження, коли критичну подію можна пропустити через розпорошеність логів.

По-третє, інфраструктурна залежність: відсутність необхідних мережевих ресурсів або уразливість самих систем моніторингу (наприклад, атака на SIEM) може поставити всю систему реагування під загрозу.

Нарешті, проблеми з інтеграцією: стандартні інструменти не завжди легко поєднуються між собою, і часто потрібні додаткові зусилля для налаштування SOAR-скриптів чи коректного збору даних із SCADA. У кризових умовах ці недоліки загострюються – наприклад, згідно з аналізом українських експертів, теперішня система сертифікації та підготовки IRT/CSIRT в Україні має «функціональні

ускладнення», і приватний сектор через недовіру до військової ієрархії не охоче ділиться інформацією з державними центрами.

Для підвищення стійкості до криз пропонують насамперед активніше використовувати штучний інтелект і машинне навчання: автоматичні механізми кореляції й аномалій, що самонавчаються, допомагають фільтрувати «шуми» та виявляти складні атаки швидше. Також корисними є кіберштабні навчання і симуляції (tabletop exercises, пентести у реальному часі), які дозволяють відпрацювати сценарії кризових реагувань і проаналізувати реакцію команди під тиском часу.

Підхід сценарного планування (як у військових ученнях) і регулярні нагальні ін'єкції інцидентів у тренувальну середу значно покращують готовність. У довгостроковій перспективі рекомендується розробка гнучкої архітектури кіберзахисту з модульними, взаємодіючими компонентами, яка б поєднувала найбільш ефективні елементи SOC, SIEM і SOAR у єдиний процес реагування.

ВИСНОВКИ ДО РОЗДІЛУ 3

Існуючі методи реагування у кризових умовах демонструють високу результативність лише за умови узгодженої роботи організаційних підрозділів та технологічних засобів. Наприклад, інтегровані підходи SOC–SIEM–SOAR забезпечують комплексне бачення ситуації: SIEM виявляє і надає дані, SOAR автоматизує дію, а SOC/CSIRT координує процес і приймає кінцеві рішення. Однак, як показано, без гнучких моделей прийняття рішень та високого рівня автоматизації залишаються «вузькі місця»: ручна обробка інцидентів і фрагментованість даних гальмують швидкість реагування. Дані методи підтверджують як фахові дослідження, так і практична аналітика: сучасним SOC потрібні AI/ML-інструменти і вдосконалення процесів, аби оперативно вирішувати завдання під час кіберкриз.

РОЗДІЛ 4
УДОСКОНАЛЕННЯ МЕТОДИКИ ТА РОЗРОБКА МОДЕЛІ УПРАВЛІННЯ КІБЕРІНЦИДЕНТАМИ В КРИЗОВИХ СИТУАЦІЯХ

4.1. Задачі та критерії ефективності моделі

Централізована система моніторингу (SIEM) є ключовим інструментом на кожному з етапів цикла реагування на інциденти інформаційної безпеки. За моделлю NIST/SANS, процес реагування складається з фаз *підготовки*, *виявлення та аналізу, стримування, ліквідації, відновлення* і *дії після інциденту*.

SIEM Graylog на кожній з цих стадій відіграє ролі

- Виявлення (Detection) та аналіз (Analysis). Саме сюди SIEM робить найбільший внесок. У фазі виявлення SIEM збирає та фільтрує мільйони подій у пошуках тих, що можуть свідчити про інцидент. Правильно налаштована SIEM генерує сповіщення про підозрілу активність у режимі реального часу. Наприклад, Graylog може відправити оповіщення на email або в Telegram при спрацюванні правила “виявлено більше 5 невдалих логінів за хвилину” чи “отримано IDS-попередження критичного рівня”. Це є сигналом до активації команди реагування. У фазі аналізу SIEM надає аналітикам інструменти розслідування: пошук за логами, побудову часових ліній подій, зведення різних джерел інформації. Завдяки централізації логів, спеціаліст з безпеки може швидко отримати відповідь на питання *«що сталося?»* – наприклад, простежити, які дії передували інциденту, які системи залучені, які облікові записи використовувалися. SIEM виступає в ролі “єдиного достовірного джерела” (single source of truth) під час початкового аналізу. Вона містить як журнали атак, так і системні логи, що допомагають зрозуміти масштаб та вплив. В Graylog можуть бути налаштовані розумні сповіщення та “плейбуки” – наприклад, при інциденті типу *malware outbreak* система одразу додає важливі поля, хеші файлів, IP командного серверу та посилання на бази Threat Intelligence для пришвидшення аналізу [22].

- Стримування *(Containment).* На цій стадії головна мета – зупинити розповсюдження інциденту, ізолювати уражені системи. SIEM допомагає ухвалити правильні рішення для стримування, надаючи актуальну картину подій. На основі даних SIEM можна швидко визначити, *які саме вузли* скомпрометовані. Наприклад, бачимо, що атакуючий IP спілкувався з двома серверами – їх і варто ізолювати від мережі. Graylog в процесі стримування використовується для пошуку IoC по всій інфраструктурі. Команда реагування може швидко прогнати індикатори (IP, хеші, домени) через всі логи, щоб знайти інші сліди присутності ворога. Ще одна важлива роль SIEM – збереження доказів. В ході стримування може знадобитися вимкнути системи або почистити їх, але вся інформація про інцидент вже зафіксована в журналах SIEM. Таким чином, навіть відключивши скомпрометовані машини, аналітики не втрачають дані про перебіг атаки. В Graylog або суміжних системах, наприклад, SOAR, інтегрованих з SIEM можливе налаштування напівавтоматичних дій стримування, таких як скрипт блокування IP на фаєрволі або відключення облікового запису в AD може бути запущений безпосередньо з консолі SIEM при підтвердженні інциденту. Це значно скорочує час реакції. Загалом, на етапі стримування SIEM виконує роль командного центру, звідки координуються всі дії.
- Ліквідація *(Eradication).* Після локалізації потрібно усунути причину інциденту, видалити шкідливе ПЗ, закрити вразливість, змінити скомпрометовані паролі. SIEM на цьому етапі підтверджує, що усунення було успішним. Наприклад, після ліквідації аналітик моніторить логи на припинення попереджень IDS, генерацыю аномальних спроб доступу. Graylog допомагає “відмотати” історію інциденту, щоб переконатися, що всі кроки ліквідації виконано. Якщо в ході аналізу виявлено, що зловмисник використовував декілька точок входу, SIEM дозволяє відстежити усі – щоб жоден backdoor не лишився. Наприклад, шляхом пошуку по логах можна знайти усі місця, куди атакувальник завантажив свої скрипти, і прибрати їх. Ще SIEM корисна для оцінки повноти ліквідації. Після застосування патчів або конфігураційних змін Graylog контролює, чи не повторюється аналогічна підозріла активність. Якщо система “затихла” – це ознака, що зловмисник більше не має доступу. У разі необхідності SIEM-логи можуть передаватися в цифрову

криміналістику – для глибшого аналізу шкідливого коду чи дій нападника, аби точно вилучити все, що він міг залишити [15].

- Відновлення *(Recovery).* Після ліквідації загрози, необхідно повернути системи до нормальної роботи. Це може включати перезавантаження серверів, відновлення даних з резервних копій, зняття ізоляції з раніше відключених вузлів. SIEM на цьому етапі продовжує моніторинг з особливою ретельністю. Відновлені системи відстежуються на предмет повторної появи ознак компрометації. Наприклад, якщо зловмисник спробує знову проникнути або якийсь компонент атаки не був повністю видалений, Graylog негайно сповістить про рецидив (через ті ж правила кореляції). Таким чином, SIEM виступає гарантом того, що *«все чисто»*. Також у фазі відновлення SIEM може генерувати звіти про інцидент для керівництва або перевірки. В звіт може входити інформація про те скільки часу зайняло виявлення (MTTD) та реагування (MTTR), які дані постраждали. Вбудовані звітні можливості Graylog дозволяють задокументувати інцидент для подальшого аналізу або виконання регуляторних вимог.
- Аналіз уроків *(Lessons Learned).* Завершальною, але надзвичайно важливою фазою є ретроспектива інциденту – аналіз того, що спрацювало добре, а що потребує поліпшення. SIEM тут забезпечує фактичний матеріал для розбору. У Graylog зберігається повний журнал розвитку подій, тому команда може крок за кроком відновити хронологію, коли відбулась перша підозріла подія, як на неї відреагували системи, які сповіщення були отримані і чи були пропущені якісь сигнали.

Наприклад, може виявитись, що SIEM згенерувала алерт, але він був класифікований як низький пріоритет і тому проігнорований – тоді варто налаштувати пріоритезацію правил. Або, навпаки, інцидент не був виявлений на ранній стадії – значить, треба додати нові кореляційні правила чи підключити додаткові джерела логів. Засвоєні уроки обов’язково документуються. SIEM може допомогти автоматизувати створення пост-інцидентного звіту. Використати збережені дані, щоб згенерувати часову діаграму атаки, виявити слабкі місця у захисті. Наприклад, якщо атака пройшла через уразливий сервер – вжити заходів

оновлення ПЗ, увімкнути сканування вразливостей. Якщо було запізніле реагування – можливо, треба поліпшити процедури оповіщення, додати дублікат тривоги у SMS [23].

Процес «lessons learned» перетворює конкретний інцидент на покращення системи безпеки. На основі логів SIEM оновлюються правила кореляції Graylog щоб подібна атака в майбутньому була виявлена на ранньому етапі та операційні плани реагування. Таким чином, з кожним інцидентом кіберстійкість організації зростає.

Отже, SIEM відіграє центральну роль у всьому циклі реагування. Від моменту виявлення, широкого охоплення й сигналізації до післяінцидентного аналізу та надання даних і контексту для висновків. У контексті Держспецзв'язку, де час реагування та координація дій критично важливі, наявність потужної SIEM-системи такої як Graylog дозволяє вибудувати чіткий процес реагування згідно з нормативними вимогами і передовими практиками (NIST SP 800-61, DSTU ISO/IEC 27035) [1].

4.2. Архітектура моделі, методи фіксації та реєстрації інцидентів

Метою методики є уніфікація фіксації подій безпеки, атак і інцидентів у масштабі установи, забезпечення достовірної доказової бази, простежуваності управлінських рішень і відповідності нормативним вимогам, що висуваються до суб'єктів у сфері захисту критичної інформаційної інфраструктури. Її дія поширюється на всі інформаційно-комунікаційні системи, сервіси, мережеві сегменти та підрозділи, включно з підрядниками, якщо вони обробляють або передають інформацію установи. Для цілей цієї методики подією безпеки вважається будь-який зафіксований факт, пов'язаний із захистом інформації (зміна політики доступу, спрацювання засобу захисту, спроба автентифікації тощо).

Інцидентом є подія або сукупність подій, що призвели або можуть призвести до порушення конфіденційності, цілісності, доступності, автентичності, підзвітності чи невідмовності. Атака визначається як навмисна дія зловмисника, спрямована на порушення одного або декількох зазначених атрибутів безпеки. Артефактами та

доказами вважаються журнали, дампи пам’яті, мережеві трасування, зразки файлів, скриншоти, електронні повідомлення, конфігурації та інші матеріали, що підтверджують обставини подій.

Відповідальність у межах процесу розподіляється таким чином. Власник активу або сервісу підтверджує критичність і межі прийнятних ризиків, погоджує пріоритети реагування та забезпечує доступ до необхідних ресурсів. Операційний центр кібербезпеки або група реагування на інциденти здійснює прийом повідомлень, класифікацію, ескалацію і координацію технічних та організаційних дій до повного закриття інциденту; веде реєстр справ у системі обліку, забезпечує безперервну комунікацію між учасниками та зберігає цілісність доказової бази.

Адміністратори систем, мереж і баз даних готують журнали та конфігурації, виконують дії стримування, ліквідації та відновлення за погодженими планами реагування. Відповідальні за комплаєнс і правовий супровід визначають необхідність та порядок повідомлення компетентних органів і партнерів, а також узгоджують правові аспекти обробки персональних даних. Окремо визначається порядок офіційних комунікацій, у тому числі зовнішніх, що здійснюються уповноваженими представниками після стабілізації ситуації [7].

Методика передбачає опору не лише на консолідацію журналів у SIEM, а й на повноцінний інструментальний ландшафт. Система обліку інцидентів (ITSM/IRP або SOAR) використовується як єдиний реєстр подій і рішень із фіксацією відповідальних осіб, строків та узгоджених дій. Сховище доказів функціонує в режимі захищеного доступу з контролем цілісності на основі криптографічних хешів і веденням журналу доступу, що забезпечує дотримання принципу непорушності ланцюга зберігання (chain of custody). Окремо підтримується сховище артефактів цифрової криміналістики для зразків шкідливого коду, образів дисків і мережевих відбитків (PCAP) з уніфікованими метаданими.

Для підвищення точності і швидкості підтвердження інцидентів використовується розвідка кіберзагроз з підтримкою обміну індикаторами компрометації у стандартах STIX/TAXII та маркуванням за моделлю TLP. Усі

джерела журналів синхронізуються зі службою точного часу (NTP) із допуском розсинхронізації, що не впливає на коректність побудови часових ліній подій.

Політика журналювання встановлює перелік обов'язкових джерел: операційні системи (Windows Event Log, Syslog), мережеве обладнання та фаєрволи, веб-фаєрволи і проксі, поштові шлюзи, засоби захисту кінцевих точок (EDR/антивірус), VPN і системи керування доступом (IAM/AD), прикладні журнали баз даних і веб-серверів, хмарні сервіси. Дані нормалізуються із застосуванням уніфікованої схеми полів, що включає, зокрема, часову мітку в UTC, атрибути джерела і призначення (адреси, порти), ідентифікатори користувачів та об'єктів, тип дії, результат та рівень суворості.

Для зовнішнього обміну і внутрішнього розмежування доступу застосовується маркування чутливості. Мінімальні строки зберігання журналів та справ встановлюються з урахуванням вимог, що висуваються до суб'єктів критичної інфраструктури, і не можуть бути меншими за один рік, якщо інше не визначено нормативно-правовими актами або внутрішніми положеннями. Цілісність журналів підтверджується періодичним хешуванням і вибірковими перевірками [24].

Для уніфікації аналізу застосовуються загальновизнані таксономії. Події та інциденти мапуються на тактики і техніки MITRE ATT&CK з метою відтворення повного ланцюга дій зловмисника та виявлення прогалин у контролях. Для статистичної звітності використовується структурований опис характеристик інцидентів (тип вектора, актори, активи, наслідки), що забезпечує порівнюваність даних між підрозділами та у динаміці. Активи класифікуються за критичністю й зонами довіри з прив'язкою до власників, що спрощує пріоритизацію реагування.

Життєвий цикл реєстрації починається з виявлення або надходження повідомлення. Джерелами ініціювання можуть бути автоматичні оповіщення засобів захисту, сигнали систем спостереження за продуктивністю, звернення користувачів, а також повідомлення від зовнішніх суб'єктів, включно з національним центром реагування. SOC/CSIRT здійснює первинний тріаж у визначені строки, залежно від попередньої суворості події, перевіряє наявність дублів, встановлює статус «подія» або «інцидент» з урахуванням впливу на активи та ймовірності ескалації, визначає

пріоритет і реєструє справу в системі обліку з присвоєнням унікального ідентифікатора, призначенням відповідального та фіксацією строків реагування.

На етапі збору доказів формується повний набір матеріалів за узгодженим часовим вікном, куди входять журнали з релевантних джерел, мережеві відбитки, конфігураційні файли, зразки файлів і, за потреби, результати «гарячої» криміналістики (дампи оперативної пам’яті, образи дисків). Усі артефакти одразу піддаються хешуванню і поміщаються до захищеного сховища із веденням журналу доступу [2].

Аналітичний етап полягає у побудові часової осі подій, мапуванні на MITRE ATT&CK, визначенні масштабу інциденту, активів, облікових записів і даних, а також у попередній оцінці правових та регуляторних наслідків. За результатами аналізу виконується ескалація відповідно до матриці ескалації: інформуються технічні та управлінські ланки, за необхідності залучаються підрозділи правового забезпечення і зовнішні компетентні органи. Усі повідомлення здійснюються через визначені канали з дотриманням вимог до захисту інформації та маркуванням ступеня поширення.

Реагування реалізується у встановленій послідовності: стримування, ліквідація, відновлення. Стримування передбачає оперативну ізоляцію уражених вузлів, блокування скомпрометованих облікових записів, застосування тимчасових правил фільтрації та обмежень доступу. Ліквідація включає усунення кореневих причин інциденту: встановлення виправлень, видалення шкідливих компонентів, вилучення закріплень, ротацію секретів і ключів. Відновлення здійснюється контрольовано, поетапно, із підвищеним моніторингом до стабілізації та підтвердження відсутності повторних ознак компрометації. Кожен виконаний крок документується в картці інциденту із зазначенням часу та відповідальних осіб, а також посиланнями на відповідні докази.

Закриття справи супроводжується обов’язковим підсумковим звітом з аналізом уроків. У звіті фіксуються виявлені сильні й слабкі сторони реагування, даються пропозиції щодо вдосконалення організаційних і технічних заходів, оновлюються плейбуки та правила кореляції, формуються нові індикатори для проактивного

моніторингу. За результатами підсумкового аналізу оновлюються ризик-реєстр і карти контролів, а також плануються цільові навчання персоналу.

Якість процесу оцінюється за показниками середнього часу виявлення та реагування, частки інцидентів, опрацьованих у межах визначених строків, повторюваності інцидентів і повноти заповнення карток. Додатково контролюється якість даних журналювання, зокрема частка нормалізованих записів і точність часової синхронізації. Плейбуки реагування та сценарії взаємодії підлягають періодичному перегляду і випробуванню у форматі навчань та настільних вправ.

Питання зберігання, приватності та відповідності вимогам регуляторів врегульовуються окремими внутрішніми документами, що встановлюють строки зберігання журналів і справ, порядок доступу за ролями, мінімізацію персональних даних у звітності та періодичні аудити практик зберігання і обробки. Таким чином описана методика забезпечує цілісний, відтворюваний і контрольований процес реєстрації атак та інцидентів, який інтегрує інструменти моніторингу, розвідки загроз, цифрової криміналістики та управління інцидентами, а також відповідає потребам захисту критично важливих активів державного сектору.

На рисунку 4.1 представлено узагальнену архітектуру методів та моделей реєстрації кібернетичних атак, яка відображає повний ланцюг обробки подій безпеки — від джерел даних і методів їх збору до етапів аналізу, прийняття рішень та формування результатів реагування. Схема демонструє поєднання сигнатурних, кореляційних, поведінкових та машинно-навчальних підходів із використанням контекстної інформації для підвищення точності виявлення та класифікації інцидентів.

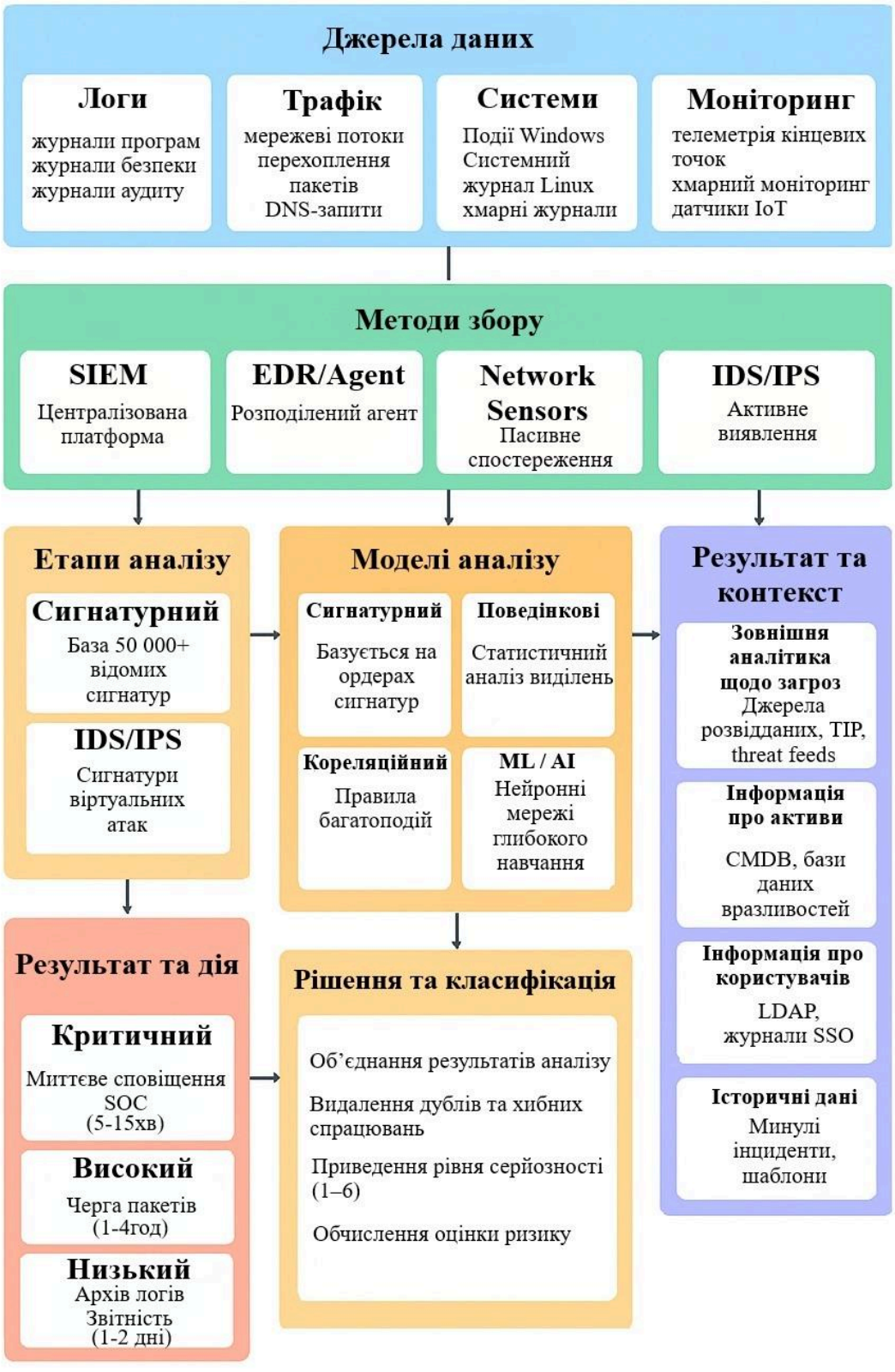

Рис. 4.1. Методи та моделі реєстрації атак

SIEM (Security Information and Event Management) платформа, така як Graylog, централізує збір журналів (логів) від різних компонентів IT-інфраструктури і

застосовує кореляційні правила для виявлення інцидентів. Щоб ефективно фіксувати атаки, SIEM отримує події з широкого спектру джерел, міжмережевих екранів (фаєрволів), систем IDS/IPS, серверів (Windows Event Log, Syslog з Linux), мережевого обладнання (маршрутизатори, комутатори), систем автентифікації (контролери домену Active Directory, RADIUS), антивірусів, веб-проксі, тощо. Кожен з цих компонентів генерує власні журнали подій, які доставляються до SIEM для зберігання та аналізу.

Для того щоб журналізувати атаки, SIEM повинна отримувати релевантну інформацію про усі ключові події безпеки. Цього досягають налаштуванням агентів або систем логування на кожному вузлі.

Перелік вузлів логування:

- Unix/Linux-сервери надсилають системні логи (про роботу служб, авторизації, ядра, мережі) через протокол Syslog (UDP/TCP) або через агенти типу Beats (Filebeat, Auditbeat), що шлють дані у форматі JSON/GELF.
- Windows-системи – використовується збір Windows Event Logs (події безпеки, системні, додатків) через спеціалізовані коннектори (наприклад, Winlogbeat, NxLog) з відправкою у форматі GELF або переведення у Syslog-формат.
- Мережеві пристрої та брандмауери – мають вбудовану підтримку Syslog і надсилають повідомлення про з’єднання, блокування трафіку, спрацювання правил захисту.
- IDS/IPS-системи (наприклад, Snort, Suricata) – можуть писати детальні журнали про кожен спрацюваний сигнатурний правил: включно з міткою часу, описом атаки, IP-адресами джерела й призначення, номером порту, пріоритетом події. Ці журнали також пересилаються у SIEM.
- Інші системи безпеки (антивірус, DLP, VPN) – генерують події про виявлення шкідливих файлів, порушення політик, підключення користувачів, тощо.

Структура логів у SIEM, як правило, уніфікована для полегшення аналізу. Graylog, зокрема, використовує структуровані формати на кшталт GELF (Graylog Extended Log Format) та підтримує JSON. Це означає, що кожне повідомлення журналу містить стандартизовані поля, такі як часова мітка, хост-джерело,

пріоритет/рівень (Info, Warning, Error, Critical), тип події, текстове повідомлення, а також додаткові поля , наприклад IP-адреси, назви процесів, коди помилок, тощо. Якщо логи надходять у неструктурованому форматі, SIEM може виконувати **парсинг** – тобто розбір тексту на складові для заповнення стандартних полів. Цей процес називається **нормалізацією логів**, різнорідні записи різних систем приводяться до спільного вигляду для спрощення пошуку і кореляції

Приклади журналів безпеки, що фіксують атаки:

```
Feb 10 15:23:45 FW01 firewall: DROP TCP 203.0.113.5:445 -> 192.168.10.5:135 FLAG:S
```

Рис. 4.2. Журнал брандмауера (Syslog)

10 лютого 15:23 FW01 зафіксував спробу підключення по TCP з підозрілого зовнішнього IP 203.0.113.5 до внутрішнього 192.168.10.5 на порт RPC 135 – з'єднання було блоковано. Така подія може свідчити про сканування портів або пошук відкритих Windows-сервісів.

```
Event ID 4625 - An account failed to log on.
User: WIN-DC\admin; Workstation: PC01; Source IP: 203.0.113.5
Failure Reason: Unknown user name or bad password.
```

Рис. 4.3. Системний журнал Windows (Security Event Log)

Невдала спроба входу під обліковим записом admin на контролері домену від імені станції PC01 з IP-адреси 203.0.113.5. Така серія подій (особливо множинні 4625 підряд) може означати брутфорс-атаку перебору паролів. SIEM збирає всі ці події і може згенерувати інцидент, якщо число невдалих логонів перевищить певний поріг.

Усі наведені приклади, потрапляючи в SIEM, мітяться часовими мітками і зберігаються для подальшого аналізу. Аналітик у SIEM може виконувати пошук за різними полями, IP-адресою, ім'ям користувача, кодом події, створювати дашборди або отримувати сповіщення про такі події. Наприклад, у Graylog можна налаштувати Stream або простий пошуковий запит на зразок:

```
source_ip: "203.0.113.5" AND event_type: "failed_login"
```

Рис. 4.4. Налаштування пошукового запиту на невдалі спроби входу

Таким чином, методи фіксації атак у SIEM полягають у всеосяжному збиранні даних з усіх можливих точок контролю, нормалізації цих даних та побудові правил, що розпізнають підозрілі шаблони у потоці подій. SIEM перетворює нескінченний потік розрізнених логів на структуровану базу знань про діяльність в мережі, з якої можна виокремити індикатори атак і своєчасно їх нейтралізувати.

Graylog, як і більшість SIEM-систем, оперує записами журналів у структурованому форматі. Основним внутрішнім стандартом Graylog є GELF (Graylog Extended Log Format) – розширений формат, спеціально розроблений для подолання обмежень класичного Syslog, що збільшив довжину повідомлення до 1024 байт та додав структуровані поля. GELF-повідомлення та інші структуровані формати, зазвичай JSON, CEF містять набір стандартних полів події, серед яких:

- timestamp – час генерації події (з точністю до мілісекунд, у UTC),
- source (host) – ім’я хоста або пристрою, що згенерував лог,
- facility/adapter – джерело або компонент (наприклад, WindowsSecurity, sshd, firewall),
- severity/level – рівень важливості (0 – Emergency, 1 – Alert, 2 – Critical, 3 – Error, 4 – Warning, 5 – Notice, 6 – Informational, 7 – Debug),
- short_message – короткий опис події,
- full_message – розгорнутий текст (якщо є),
- унікальний ID (наприклад, _id у Graylog) та інші.

Крім того, Graylog дозволяє доповнювати запис довільними полями, префіксованими знаком підкреслення, наприклад, _src_ip, _dst_port, _username. Це означає, що під час прийому логів можна налаштувати парсинг, який виділить з тексту повідомлення значущі атрибути і збереже їх як окремі поля. Наприклад, для IDS-попередження доцільно мати поля src_ip, src_port, dst_ip, dst_port, alert_signature, priority. Для Windows-логів – event_id, user, domain, status_code.

Типи подій, за якими в Graylog вибудовується моніторинг безпеки:

- Аутентифікація та авторизація, яка визначає успішні та неуспішні спроби входу (Event ID 4624, 4625 у Windows; відповідні повідомлення PAM у Linux), блокування облікових записів, зміна паролів, ескалація привілеїв (наприклад, додання користувача до адміністраторів).
- Доступ до критичних ресурсів, події доступу до конфіденційних файлів або областей системи (FileAudit, Object Access), запуск важливих служб, підключення до баз даних, використання команд адміністрування.
- Мережеві підключення, такі як відкриття/закриття з'єднань, відхилені фаєрволом пакети, нетиповий трафік (наприклад, великі обсяги вихідних даних у незвичний час), зміни у таблицях маршрутизації або конфігурації мережі.
- Попередження систем захисту які фіксують спрацювання IDS/IPS правил (атакуючі IP, сигнатури), виявлення вірусів антивірусом, блокування небезпечних веб-запитів WAF'ом, спроби підбору облікових даних (brute-force) тощо.
- Системні збої та помилки, наприклад падіння критичних сервісів, BSOD/kernel panic, множинні помилки додатків – інколи саме такі технічні збої можуть бути наслідком атаки.
- Зміни конфігурацій, таких як встановлення нового ПЗ, внесення змін у системні файли, активація/деактивація мережевих інтерфейсів, вимкнення журналювання чи засобів безпеки.
- Інші аномалії, наприклад, аномальні часові патерни (спроби входу у нетиповий час доби), аномальні локації (вхід користувача з IP іншої країни), аномалії цілісності (зміна контрольних сум файлів).

Graylog надає гнучкі засоби для класифікації подій. За допомогою Streams можна розподілити потоки логів за категоріями, наприклад, потік "Атаки" – всі події IDS і фаєрволів; потік "Аудит AD" – події Windows AD. Це дозволяє застосовувати до кожної категорії свої правила кореляції та сповіщення. Крім того, визначення подій (Event Definitions) дають можливість задати умови, за яких із сирих логів генерується особлива "подія безпеки" у Graylog. Наприклад, можна створити подію "MassiveFailedLogons", яка спрацьовує, якщо протягом 1 хвилини виявлено понад 10

невдалих логонів одного користувача. Подібні механізми фільтрації та агрегування даних в Graylog дозволяють зосередитися на дійсно важливих інцидентах, відсіваючи “шум” інформаційних і службових повідомлень.

Розглянемо приклад процесу атаки, яку може виявити IDS/IPS. Щоб продемонструвати взаємодію компонентів захисту, розглянемо сценарій складної атаки на корпоративну мережу, визначимо на яких етапах IDS/IPS, інші засоби її виявлять:

Етап 1: Розвідка (Reconnaissance). Зловмисник починає з дальньої розвідки мережі. Він може використовувати сканери портів, таких як Nmap для виявлення активних хостів і відкритих сервісів. В нашому випадку атакуючий з IP 203.0.113.5 проводить сканування діапазону IP корпоративної мережі.

- *Детектування відбувається на основі м*ережевої IDS, розгорнута на периметрі, фіксує аномальну кількість запитів з однієї адреси на різні порти. У базі сигнатур IDS присутні правила, що розпізнають типовий шаблон сканування Nmap. Як результат, IDS генерує попередження: “Possible Portscan from 203.0.113.5” (з детальним списком цілей та портів). Graylog отримує ці логи, і на їх основі можна побудувати дашборд активності сканування такого як, графік кількості підключень з цього IP за часом, таблиця цільових хостів. На рис.4 практичної частини якраз проілюстровано виявлення OpenVAS-сканування через Graylog.

Етап 2: Експлуатація вразливості (Exploitation). Після збору інформації зловмисник знаходить уразливий сервіс, наприклад веб-сервер з застарілою версією, що має вразливість віддаленого виконання коду. Він відправляє спеціально сформований шкідливий запит, який експлуатує цю вразливість і дає йому доступ до серверу.

- *Детектування загрози* буде простішим якщо на цьому сервері або на мережі встановлено HIDS/NIDS з відповідними сигнатурами, то сам факт експлуатації може бути спійманий. Наприклад, IDS має сигнатуру на відомий експлойт і згенерує alert “EXPLOIT Apache Struts RCE attempt” з високим пріоритетом. Якщо ж експлойт невідомий (0-day), то пряма сигнатура відсутня, але система може зафіксувати аномалію: незвичний трафік, або виконання процесу на

сервері. В журнали сервера потрапить запис про помилку або нестандартний POST-запит. У будь-якому разі, SIEM отримує або попередження IDS, або лог помилки сервера, що слугують індикаторами. Правило кореляції в SIEM може позначити таку подію як можливе успішне проникнення.

Етап 3: Закріплення та розвиток атаки (Establishment & Persistence). Отримавши доступ, зловмисник встановлює бекдор для збереження присутності – наприклад, створює нового прихованого користувача в системі або впроваджує shell для віддаленого керування. Далі він може виконувати горизонтальне переміщення: сканувати внутрішню мережу вже з компрометованого вузла, шукати інші цілі (бази даних, файлові сервери), збирати конфіденційні дані.

- *При детектуванні* на цьому етапі, цілий ряд подій може привернути увагу. IDS внутрішнього сегмента помітить, що зі взламаного сервера йде сканування по локальній мережі. Системні логи сервера реєструють появу нового облікового запису або запуск нетипової служби. Антивірус/EDR на вузлі може спіймати підозрілий виконуваний файл. SIEM здатен корелювати ці ознаки, адже одна й та ж машина протягом короткого часу згенерувала *кілька різних тривожних подій*, а саме, alert IDS, створення користувача, спрацьовування антивірусу. Це привід створити зведений інцидент високого рівня. Кореляційне правило Graylog може бути налаштоване за принципом: “Якщо на одному хості протягом 10 хвилин відбулося IDS-попередження та подія додавання адміністратора – згенерувати “**Alarm**”. Таким чином, SIEM допомагає *виявити складну багатоетапну атаку*, яку окремо взяті системи могли б частково проігнорувати.

Етап 4: Ексфільтрація та фінальна фаза (Exfiltration & Action on Objectives). Завершивши збір даних, зловмисник намагається переслати їх назовні – наприклад, упакувати та відправити на свій сервер через FTP, HTTP або навіть по DNS-тунелю. Інші можливі дії – запустити руйнівний payload, випустити ransomware, стерти дані.

- *Під час детектування* незвично великий обсяг вихідного трафіку або нестандартний протокол може бути помічений системами DLP чи мережевим моніторингом. Міжмережевий екран може згенерувати лог: “Large outbound transfer from 192.168.10.5 to 203.0.113.10 blocked”. IDS може мати правило на відомі

інструменти ексфільтрації, таких як “DNS Tunnel Usage”. Graylog на дашборді мережевого трафіку покаже пік вихідних даних. Також, після атаки, системні журнали можуть зафіксувати наступні дії, а саме шифрування файлів, що є ознакою ransomware – антивірус згенерує серію попереджень про шифрування. SIEM корелює сигнали так, що масове шифрування та зникнення файлів тіньового копіювання є інцидентом типу “Ransomware Detected”.

У підсумку, на кожному етапі комплексна система моніторингу на базі IDS та SIEM здатна або попередити атаку, або мінімізувати її наслідки. IDS/IPS виконує роль “першої лінії” – миттєво реагує на мережеві атаки, блокує або сповіщає, а SIEM – центрального аналітика, що збирає всі шматочки мозаїки воєдино. У представленому прикладі, навіть якщо окремі ознаки могли лишитися непоміченими, SIEM забезпечила **“**єдиний екран” (single pane of glass), де видно повний розвиток атаки, від сканування до ексфільтрації. Це дозволяє командам безпеки оперативно локалізувати та розслідувати інцидент.

4.3. Формальні алгоритми пріоритизації інцидентів і розподілу ресурсів

Одним із базових елементів превентивної кібербезпеки є сканування вразливостей**.** Воно призначене для проактивного виявлення слабких місць у програмному забезпеченні, мережевих службах та конфігураціях до того, як ними скористаються зловмисники. Регулярне сканування дозволяє організаціям оцінювати та вдосконалювати рівень захищеності своїх систем. Знахідки сканера допомагають командам безпеки пріоритизувати та своєчасно усувати вразливості, тим самим зменшуючи потенційну поверхню атаки і запобігаючи інцидентам витоку даних. Іншими словами, сканер діє як автоматизований аудитор безпеки**,** що систематично перевіряє IT-інфраструктуру на наявність відомих небезпечних конфігурацій, застарілого ПЗ, відомих експлойтів.

До основних переваг впровадження сканування вразливостей належать:

- Зниження ризиків: раннє виявлення та виправлення потенційних вразливостей значно зменшує імовірність успішної кібератаки.

- Підвищення безпеки: постійний моніторинг і усунення слабких місць підтримує високий рівень захищеності системи.
- Дотримання нормативів: регулярні перевірки допомагають відповідати вимогам стандартів і законодавства у сфері захисту інформації.
- Запобігання збиткам: усунення критичних дір забезпечує безперервність бізнес-процесів, захист репутації організації і економію коштів, що могли б бути втрачені через інцидент.

Для виконання сканування можуть застосовуватися як комерційні, так і відкриті інструменти (OpenVAS, Nessus, Nmap тощо). У практичних умовах Держспецзв'язку широко використовується платформа Greenbone/OpenVAS – потужний відкритий сканер, що дозволяє автоматично перевіряти вузли мережі за великою базою тестів на відомі вразливості. Результати сканування зазвичай містять перелік знайдених проблем з класифікацією за рівнем критичності та рекомендаціями щодо усунення. Таким чином, сканування вразливостей є невід'ємною складовою кіберзахисту, оскільки створює першу лінію оборони**:** виявляє та закриває "дірки" у безпеці до того, як ними скористаються зловмисники.

Атаки на інформаційні системи сьогодні набули різноманітних форм і постійно еволюціонують. Загалом їх можна поділити на декілька типових категорій:

- Соціальна інженерія та фішинг – шахрайські спроби обманом змусити користувача видати конфіденційну інформацію або виконати небезпечну дію. Ознаки: підроблені листи, повідомлення або сайти, що імітують легітимні. Механізми детектування: антифішингові фільтри в пошті та браузерах, навчання користувачів уважності.
- Шкідливе програмне забезпечення (Malware) – віруси, трояни, програм-вимагачі (ransomware) тощо, які потрапляють на систему і виконують несанкціоновані дії (шифрування файлів, крадіжка даних). Ознаки: підозрілий запуск невідомих програм, несанкціоновані зміни файлів, аномальний мережевий трафік з робочих станцій. Виявлення: антивірусні системи з сигнатурами, поведінкові аналізатори (EDR), моніторинг хешів файлів, сповіщення про шифрування великої кількості файлів.

- Атаки типу DoS/DDoS – спрямовані на відмову в обслуговуванні шляхом масового перевантаження сервера або мережі запитами. Ознаки: різкий стрибок трафіку, недоступність сервісів, вичерпання ресурсів. Детектування: мережеві монітори продуктивності, спеціалізовані системи DDoS-захисту, які фільтрують аномальний трафік.

- Атаки на веб-застосунки – SQL-ін'єкції, XSS, RCE та інші, що експлуатують вразливості у веб-сайтах і сервісах. Ознаки: незвичайні запити в логах веб-сервера (наприклад, з підозрілим payload у параметрах URL), спроби виконання стороннього коду. Виявлення: веб-фаєрволи (WAF), сигнатури IDS/IPS для відомих експлойтів веб-уразливостей, аналіз журналів доступу на аномальні шаблони.

- Цільові атаки та APT (Advanced Persistent Threat) – багатоступеневі затяжні атаки, часто спонсоровані державою або організованими групами, націлені на конкретну організацію. Вони комбінують кілька технік (фішинг для проникнення, malware для закріплення, внутрішнє переміщення в мережі, крадіжка даних). Ознаки: поодинокі на перший погляд події (наприклад, разове проникнення через spear-phishing), що ведуть до подальших тихих дій (створення бекдору, збір даних, встановлення прихованих комунікацій із командними серверами). Виявлення: аналіз кореляції подій у SIEM, використання розвідки кіберзагроз (Threat Intelligence) для відстеження індикаторів компрометації (IoC), поведінкові системи виявлення аномалій.

- Внутрішні загрози (Insider threats) – зловживання з боку внутрішніх користувачів, що мають авторизований доступ. Можуть бути як умисними (незадоволений співробітник краде дані), так і випадковими (співробітник по необережності відкрив шкідливий файл). Ознаки: нетипова активність легітимного облікового запису (наприклад, масове копіювання конфіденційних файлів, спроби доступу до незвичних ресурсів). Виявлення: відстеження поведінки користувачів та entity (UEBA-системи), контроль привілейованих дій, журналювання важливих операцій (таких як експорт даних, зміни прав тощо).

Системи виявлення вторгнень (IDS/IPS) теж адаптуються до новітніх атак. Окрім сигнатурних правил, сучасні IDS використовують евристики та машинне

навчання для фіксації відхилень від нормально поведінки мережі. Наприклад, аномально високе число запитів або поліморфні пакети можуть бути класифіковані як підозрілі навіть без явної сигнатури. Таким чином, комплексне застосування інструментів IDS, аналізаторів поведінки, SIEM дає змогу фіксувати як відомі типи атак, так і нові, ще не описані загрози.

Процес реалізації сучасної цілеспрямованої атаки на корпоративне середовище, зокрема на об'єкт критичної інформаційної інфраструктури, доцільно описувати як послідовність взаємопов'язаних етапів, кожен з яких породжує характерні технічні ознаки у журналах подій та піддається контролю за допомогою засобів виявлення вторгнень і систем централізованого моніторингу. Типова траєкторія включає розвідку, експлуатацію вразливості, закріплення та розширення присутності зловмисника, ексфільтрацію даних або інші дії над цілями.

На етапі розвідки зловмисник збирає відомості про інфраструктуру цілі: діапазони адрес, доступні служби, версії програмного забезпечення, топологію та потенційні точки входу. У мережевому вимірі це проявляється у вигляді систематичного опитування вузлів й портів, збільшеної частоти спроб установлення з'єднання до нетипових сервісів, появи запитів з нерепрезентативних для організації географічних регіонів, а також у вигляді специфічних «почерків» сканерів.

У журналах брандмауера та мережевих датчиків IDS фіксуються відхилені або дозволені спроби доступу з однієї й тієї самої адреси джерела до великої кількості призначень і портів за короткий проміжок часу; у системних журналах серверів можуть з'являтися записи про нестандартні заголовки запитів до веб-інтерфейсів або про багаторазові спроби зчитування публічних сторінок із параметрами, що не властиві звичайному користуванню. На цьому етапі первинний контроль реалізується шляхом виявлення аномальної частоти з'єднань, сплесків трафіку до рідкісних портів, а також кореляції подій з однієї адреси джерела у вікні часу, визначеному політикою моніторингу. За наявності централізованого журналювання SIEM формує інформативну часову лінію активності, що надалі використовується як доказова база.

Експлуатація вразливості є моментом переходу від розвідки до власне вторгнення. Зловмисник застосовує відомий або невідомий (нульового дня) механізм

для виконання коду, підвищення привілеїв або обходу автентифікації. Технічно це супроводжується появою у журналах веб-серверів запитів із навмисно зміненими параметрами, у системних журналах — записів про аварійні завершення процесів або створення нетипових дочірніх процесів від імені системних служб, у засобах захисту кінцевих точок — спрацьовуваннями щодо підозрілої поведінки або завантаження виконуваних модулів із невідомими контрольними сумами.

У середовищах на базі доменної інфраструктури фіксуються збиті або неуспішні спроби входу, а також подальші раптові успішні входи для облікових записів, що раніше не проявляли активності на даному вузлі. Засоби IDS/IPS здатні виявляти типові послідовності пакетів і сигнатури для поширених експлойтів; у випадках, коли сигнатури відсутні, вирішальну роль відіграє поведінковий аналіз і кореляція подій у SIEM: поєднання відмов у доступі, системних помилок і різкої зміни профілю з'єднань служить підставою для класифікації інциденту як проникнення.

Закріплення та розширення присутності охоплює дії зловмисника, спрямовані на збереження контролю над середовищем і горизонтальне переміщення. Практично це виявляється у створенні нових або модифікації наявних облікових записів, додаванні користувачів до груп із підвищеними правами, внесенні змін до планувальників завдань і служб автозапуску, встановленні додаткових компонентів віддаленого керування, використанні законних інструментів адміністратора для ускладнення виявлення. У мережевому трафіку з'являються регулярні сесії до зовнішніх вузлів керування, а всередині сегментів — внутрішнє сканування та підключення до служб, які не входять до типового профілю взаємодії конкретного сервера чи робочої станції.

У журналах безпеки фіксуються події створення або зміни облікових записів, успадкування привілеїв, нетипові звернення до каталогів керування доменом та об'єктів групової політики. Для мінімізації часу прихованої присутності використовуються кореляційні сценарії: якщо на одному вузлі протягом визначеного вікна часу виявлено попередження IDS щодо підозрілої взаємодії, подію підвищення

прав доступу та появу нового мережевого з’єднання до недекларованого зовнішнього ресурсу, інцидент підлягає негайній ескалації із застосуванням заходів стримування.

Ексфільтрація даних та інші дії над цілями становлять завершальну фазу атаки, у межах якої відбувається виведення конфіденційної інформації, руйнування або шифрування даних, порушення доступності сервісів. Журнали мережевих пристроїв і систем виявлення фіксують нетипові обсяги вихідного трафіку, нестандартні для організації протоколи або тунелювання поверх протоколів доменної служби і системного іменування, звернення до ресурсів із переліків загроз. У журналах файлових систем і прикладних сервісів з’являється масове створення або зміна файлів, ознаки шифрування, відключення тіньового копіювання, модифікація політик доступу, зупинка критичних служб. На цьому етапі технічний контроль поєднується з організаційними діями: ізоляція сегментів і вузлів, блокування облікових записів, застосування політик заборони вихідних з’єднань за «білим» переліком, активація планів відновлення та резервного копіювання. Централізоване журналювання надає можливість відновити повну хронологію, визначити обсяг ураження та підтвердити завершення ексфільтрації чи руйнівної активності.

Окремої уваги потребують випадки використання вразливостей нульового дня, коли сигнатурні ознаки відсутні. У таких ситуаціях визначальною стає наявність послідовної картини аномалій у різних доменах подій: невластиві шаблони мережевих з’єднань, зміни в моделях автентифікації та доступу, запуск невідомих процесів від імені системних служб, модифікації реєстру та планувальників завдань, а також відхилення у телеметрії засобів захисту кінцевих точок. Методично правильним є підхід, за якого всі перелічені ознаки підлягають уніфікованому журналюванню, нормалізації та кореляції, а будь-яка сукупність із двох-трьох незалежних сигналів у межах короткого часового вікна автоматично переводить справу до категорії підвищеного пріоритету з ініціюванням заходів стримування до підтвердження або спростування інциденту.

У процесі документування для кожної фази атаки має бути зазначено конкретні системи журналювання, типи подій, ключові атрибути записів, що підтвердили перехід між фазами, а також технічні та організаційні рішення, прийняті у відповідь.

Такий підхід не лише підвищує імовірність раннього виявлення та локалізації складних загроз, але й забезпечує відтворюваність і придатність матеріалів для службових перевірок та, за потреби, для подальшої правової оцінки.

4.4. Гібридна інтеграція, механізми кореляції й адаптації; комунікаційні протоколи

Однією з найсильніших можливостей SIEM Graylog є побудова кореляційних правил, що дозволяють автоматично виявляти комплексні атаки шляхом зіставлення кількох різнорідних подій. Graylog має вбудований Correlation Engine, який дає змогу визначати послідовності подій, котрі повинні відбутися в заданому часовому вікні, щоб згенерувати тривогу.

Приклади кореляційних правил які допомагають виявити складні атаки

- Кореляція по полю (Per Field Correlation). Можна згрупувати події за певним ключем IP-адреси, ім’ям користувача. Graylog дозволяє задати ключове поле і відстежувати серії подій з однаковим значенням цього поля. Наприклад, ключ – src_ip. Якщо для одного джерела протягом 5 хв зафіксовано >N різних сигнатур IDS, це може свідчити про масовану атаку під час якої зловмисник перепробує багато методів – генеруємо алерт “Мультивекторна атака з IP X”.
- Кореляція між джерелами (Cross Event Source Correlation). Це пошук патернів між подіями різних типів. Graylog дає змогу задати правило, яке зміщує акцент на послідовність: *“якщо протягом 1 хвилини після IDS-спрацювання з певного IP відбувся успішний логін на сервер – сповістити про можливий прорив”*. Таким чином, пов’язується воєдино мережевий рівень (атака) та рівень додатків (вхід), що окремо могли б загубитися серед шуму [5].
- Пошук відсутньої події (Negative Event). Вид кореляції – коли правило тригериться не на наявність чогось, а на відсутність очікуваної події**.** Наприклад, якщо після оновлення системи очікується перезапуск служби і запис у лог “Service started”, а його немає – це теж може бути ознака саботажу або збоїв. Хоч це

опосередковано стосується атак, але в комплексі відсутність логів резервного копіювання чи оновлень безпеки може вказувати на приховане втручання.

- Складна багатоступенева кореляція (Complex Correlation). Graylog дозволяє вибудовувати правила на основі вже існуючих алертів. Це фактично створення ієрархії. Наприклад, спочатку визначено подію “Brute-force attack”, окремо – подію “New Admin Account Created”. Далі можна зробити кореляцію другого рівня: *“якщо після brute-force одразу створено нового адміністратора”*. Це і буде ознака, що brute-force успішно привів до компрометації – тобто, атака пройшла увесь ланцюжок. Такий рівень кореляції виявляє цільові атаки більш надійно, ніж одновимірні сигнатури.
- Кореляція з зовнішніми даними (Threat Intelligence). Хоча це більше налаштовується окремо, але Graylog може імпортувати списки відомих шкідливих IP. Правило може бути: *“подія network_connection та IP із списку ThreatIntel = сигнал”*. Ця кореляція додає контекст до сирих логів – що підвищує виявлення APT-активності, де часто задіяні інфраструктурні сервери керування, відомі розвідці.

Налаштування кореляційних правил у Graylog здійснюється через інтерфейс Event Definitions. Там можна послідовно додати кілька умов, вказати часовий інтервал, протягом якого вони мають спрацювати, і навіть задати кількісні пороги. Наприклад Event A має статись щонайменше 5 разів, потім Event B 1 раз. Якщо всі умови виконано – генерується зведена подія (інцидент) з власним повідомленням. Такий гнучкий підхід дозволяє “упіймати” складні сценарії, які не виражаються одиничним логом.

Скажімо, без кореляції масований брутфорс – це всього лиш десятки стандартних подій, а створення нового адміністратора – одинична подія. Жодна з них поодинці не є критичною. Проте кореляція їх переводить у категорію Critical. Отже, Graylog виступає як “цифровий детектив”, що співставляє факти і робить висновок про наявність атаки. У реальних умовах Держспецзв’язку це може означати виявлення “тихих” атак. Наприклад, якщо зловмисник отримав низькорівневий доступ і повільно розвідує мережу, лише кореляція різних слабких сигналів дозволить виявити його дії, поки не стало надто пізно.

Розглянемо приклад аналітичного дашборду Graylog для візуалізації подій безпеки, який є інтерактивною панеллю моніторингу, що наочно відображає ключові метрики та події кібербезпеки в режимі реального часу. Graylog надає широкі можливості для побудови кастомних дашбордів, а саме користувач може перетягувати віджети різних типів і налаштовувати їх під свої потреби. Виглядають дані дашборди у контексті моніторингу загроз таким чином:

- Дашборд мережевих атак демонструє поточну картину сканувань, вторгнень, підозрілої активності. Тут доречно використати графіки часового ряду (Time Series) для відображення кількості різних типів алертів IDS по хвилинах/годинах. Наприклад, графік “IDS Alerts (Critical) over last 24h” з піками під час масованої атаки. Поряд можна розмістити стовпчикову діаграму “Top 10 Attacker IPs” – яка IP-адреси найчастіше траплялися в логах IDS/фаєрвола за останній тиждень. Кожна колонка – IP і кількість спрацювань. Також таблиця “Latest Critical Alerts” із переліком останніх серйозних попереджень (полями: час, джерело, опис сигнатури, ціль). Для високорівневої оцінки – єдиний показник**,** наприклад, кількість інцидентів високого пріоритету за поточну добу. Такий дашборд дозволяє черговому аналітику одразу бачити аномалії. Якщо графіки різко ростуть – атака наростає, якщо топ-атакер один і той самий – можливо, триває цільована атака з конкретного джерела [6].

- Дашборд аутентифікації і доступів виявляє спроби компрометації облікових записів та несанкціоновані доступи. Тут може бути кругова діаграма (pie chart), що показує розподіл подій входу, успішних та неуспішних за останню добу. Географічна карта з відмітками – звідки здійснювалися спроби входу. Карта допомагає побачити, якщо раптом з’явилася точка на карті далеко за межами України, звідки ніхто з персоналу не мав би мати доступу в корпоративну мережу. Таблиця “Account Lockouts Today” – список користувачів, чиї облікові записи блокувалися. Лінійний графік “VPN Logins per Hour” – для моніторингу віддалених підключень. Цей дашборд дозволяє відповідальному за IDM (управління доступом) оперативно бачити підозрілий сплеск невдалих логінів або незвичну географію логінів.

- Дашборд цілісності та шкідливого ПЗ виявляє інциденти з використанням неузгодженого програмного забезпечення. На ньому можна розмістити теплову карту, що відображає за останній місяць дні і часи, коли спостерігалися інциденти з malware (чим червоніше поле – тим більше подій того дня/години). Стовпчикова діаграма “Types of Malware Detected” – показує, яких категорій загрози траплялися і їх кількість. Цей дашборд дає змогу оцінювати ефективність антивірусного захисту та тенденції заражень.

Всі дашборди Graylog підтримують оновлення в реальному часі та взаємодію з користувачем. Це означає, що аналітик може використовувати їх не лише для пасивного спостереження, а й для розслідування, відфільтрувати один графік за конкретним IP та автоматично побачити, як інші графіки перебудуються для цього IP.

Окремо слід зазначити про готові дашборди (Graylog Illuminate) – колекцію шаблонів від виробника, які охоплюють типові потреби безпеки (виявлення загроз, відповідність вимогам, тощо). Вони можуть використовуватись як основа і налаштовуватись під специфіку Держспецзв’язку. Наприклад, для контролю відповідності вимогам можуть бути дашборди PCI DSS або НД TZI.

Таким чином, аналітичні дашборди Graylog перетворюють великий обсяг логів на зрозумілу візуальну інформацію, а саме графіки тенденцій, діаграми розподілу, карти атак. Це суттєво полегшує виявлення аномалій і дозволяє командам кібербезпеки приймати рішення оперативно та на основі даних. Для Держспецзв’язку такі засоби є невід’ємною частиною ситуаційного центру. Вони забезпечують безперервний нагляд за кіберстановищем у підпорядкованих інформаційних системах та дають можливість реагувати превентивно, ще до того як інциденти спричинять значну шкоду.

4.5 Методологія управління кіберінцидентами та експериментальна валідація розробленої моделі

Інтеграція моніторингу та виявлення загроз на базі SIEM Graylog та IDS/IPS

Об’єднання системи моніторингу та виявлення загроз у єдине корпоративне середовище має на меті скоротити час реагування на інциденти. Зокрема, використати Graylog як SIEM для централізації логів та кореляції подій від IDS/IPS, що дозволить швидко ідентифікувати та реагувати на загрози в реальному часі.

Хід виконання Завдання 1: Побудова тестового корпоративного середовища з централізованим логуванням та аналізом мережевої активності

Створення тестового корпоративного середовища на базі Windows Active Directory

На початковому етапі було розгорнуто тестове корпоративне середовище з централізованим управлінням на основі служби каталогів Windows Active Directory (AD). Цей компонент забезпечує централізовану автентифікацію, управління політиками безпеки, керування ресурсами та користувачами.

1. Створено віртуальну машину з ОС Windows Server 2022.

2. Встановлено роль Active Directory Domain Services (AD DS) та налаштовано новий домен (наприклад, corp.local).

3. Проведено ініціалізацію домену, створено контролер домену, DNS-сервер і базу даних каталогів.

4. Додано користувачів Active Directory для подальшої аутентифікації пристроїв.

5. Підключення 4 користувачів до корпоративної мережі

Було налаштовано чотири клієнтські машини:

2 Windows-клієнти Windows 10 — приєднані до домену через графічний інтерфейс:

- Вказано DNS-сервер домену.
- Приєднано систему до домену corp.local.
- Перевірено входи користувачів AD з різних машин.

2 Linux-клієнти Ubuntu 22.04 — приєднання до корпоративного середовища виконано з використанням служби SSSD:

- Встановлено пакети sssd, realmd, krb5-user, samba, adcli.

- Виконано команду realm join corp.local з обліковими даними адміністратора.
- Перевірено вхід користувача домену з терміналу Linux.

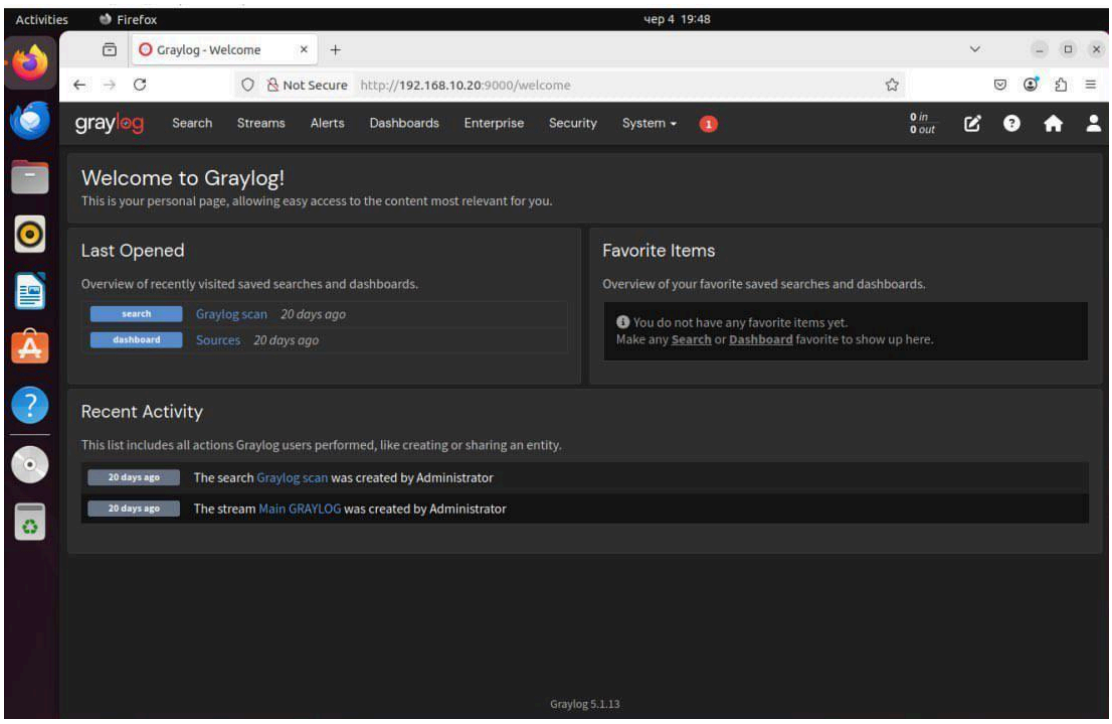

Рис. 4.5. Усі машини зареєстровані у домені, авторизація працює коректно.

Встановлення системи централізованого логування Graylog

Для централізованого збору, зберігання та аналізу логів було обрано SIEM-платформу Graylog, що підтримує масштабовану обробку логів у реальному часі.

Створено окрему віртуальну машину Ubuntu Server, на яку встановлено:

- MongoDB – база даних конфігурацій.
- Elasticsearch (OpenSearch) – система індексації логів.
- Graylog Server – основний компонент.

Налаштовано Input типу Syslog UDP (і TCP) для приймання логів з клієнтських машин. Після запуску вебінтерфейсу (http://graylog.local:9000), перевірено отримання перших логів.

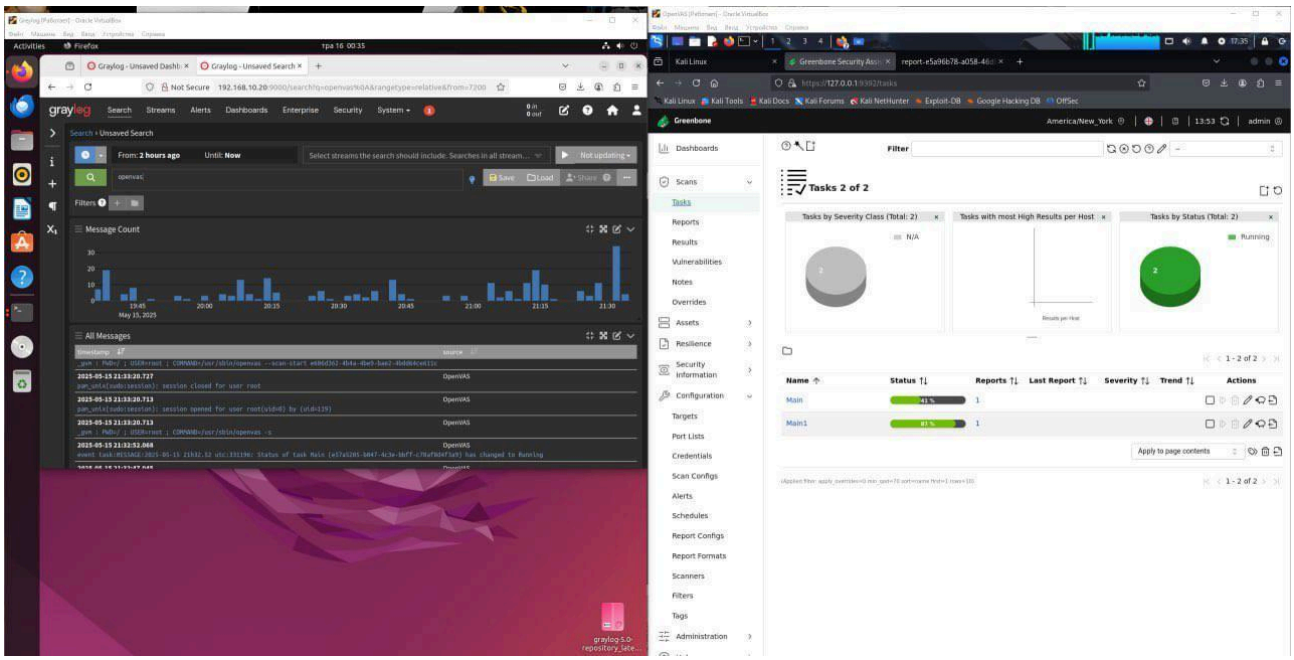

Рис. 4.6. Отримання перших логів

Налаштування збору подій з усіх машин

Windows:

- Встановлено Winlogbeat на кожному клієнті.
- Налаштовано winlogbeat.yml на відправлення логів до Graylog через Syslog.
- Запущено сервіс Winlogbeat, події почали надходити до Graylog.

Linux:

1. Встановлено rsyslog.
2. Додано конфігурацію відправки системних логів (/var/log/syslog, /var/log/auth.log) на адресу сервера Graylog.
3. Перевірено наявність подій у вебінтерфейсі Graylog, зокрема:
   - Логи SSH (успішні/невдалі входи).
   - Системні повідомлення (процеси, ядро, служби).

Graylog отримує повний набір подій з усіх 4 клієнтських машин у реальному часі.

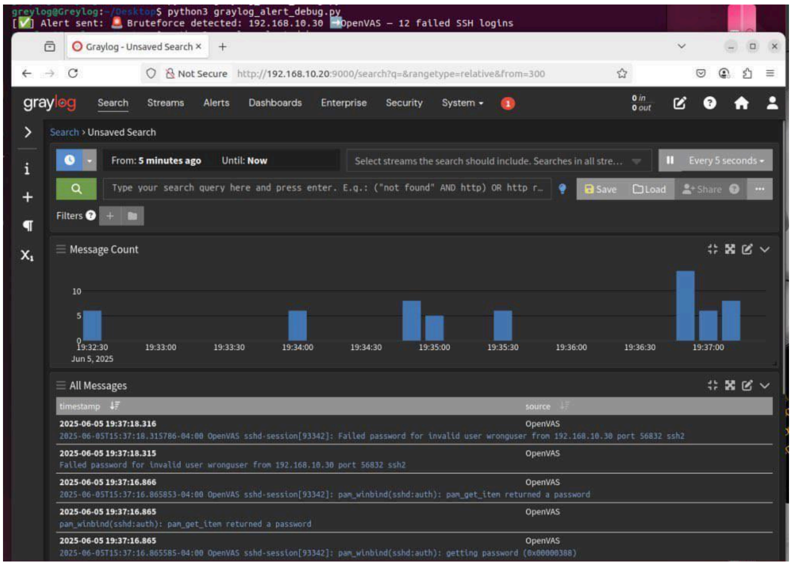

Рис. 4.7. Фіксація подій з усіх машин в мережі

Виконання сканування мережі за допомогою OpenVAS

- Для імітації зовнішньої атаки проведено сканування тестової мережі.
- Розгорнуто окрему віртуальну машину з Greenbone/OpenVAS (Kali Linux).
- Виконано повне сканування діапазону IP-адрес корпоративного середовища.

Параметри сканування: виявлення відкритих портів, служб, версій програм, перевірка на відомі вразливості.

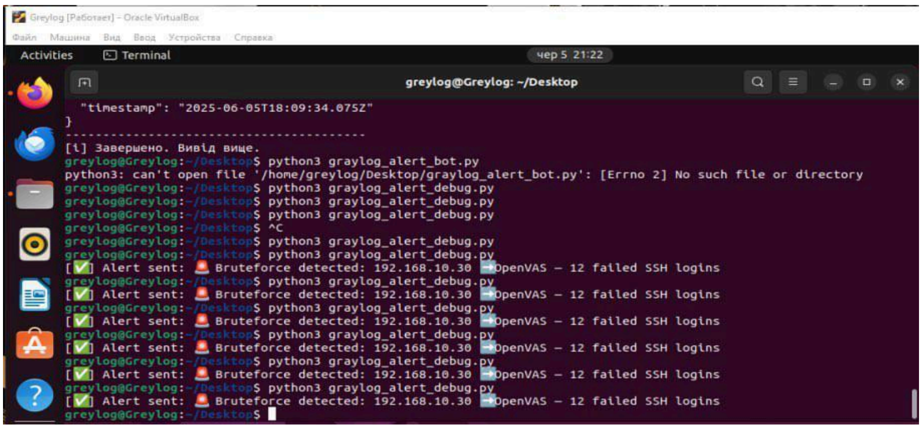

Рис. 4.8. Фіксація невдалих спроб підключення SSH

Виявлення активності сканування через лог-аналітику в Graylog

- Після запуску сканування було проаналізовано події в Graylog на предмет:
- Аномальної кількості входів з IP-адреси сканера.
- Зростання трафіку на порти, які не використовуються зазвичай.
- ICMP-запити, які використовувались під час сканування.

Використано:

- Dashboards — для візуалізації подій у часі.
- Search — для фільтрації:
- source: "192.168.1.100" AND event_type: "connection attempt"
- Створено Stream для автоматичного виділення подібних подій.

Результат: було зафіксовано кілька десятків спроб підключення до різних портів на всіх машинах. Graylog дозволив швидко ідентифікувати джерело активності (IP OpenVAS) та підтвердити факт сканування. Завдання виконано повністю. Створене середовище дозволяє:

- централізовано керувати пристроями через AD,
- збирати логи з усіх машин,
- виявляти підозрілу активність у мережі через аналіз логів у Graylog,
- здійснювати базову кореляцію подій.

Це середовище можна масштабувати для подальших експериментів з аналізу безпеки, написання скриптів автоматичного реагування, виявлення складніших атак.

Для подальшого аналізу розроблено скрипт, правило конвеєра Graylog, який автоматично витягує важливі поля з повідомлень IDS, IP-адресу джерела атаки, номер порту, тип атаки. Такий механізм аналізу дозволяє структурувати дані та виконувати пошук за певними параметрами. Наприклад, за допомогою конвеєрних правил можна вирахувати джерело атаки і встановити поле src_addr для подальшої кореляції.

Система IDS була налаштована на відправку своїх подій до Graylog через спеціальні лог-інпути чи агенти. Це забезпечило надходження повідомлень про потенційні атаки в єдину платформу, де їх можна корелювати із системними та мережевими логами. Як показано на прикладі з документації Graylog, завдяки кореляції подій IDS з іншими логами вдалося виявити невдалу атаку на SSH і

відслідкувати її наслідки. Такий підхід підвищує видимість інцидентів і дає можливість глибокого аналізу.

Для своєчасного інформування адміністратора про критичні події встановлено плагін TelegramNotification для Graylog. Після створення бота у Telegram та інтеграції з Graylog налаштовано шаблон повідомлень: при спрацьовуванні визначеної події. При високому рівні небезпеки від IDS, Graylog відправляє нотифікацію адміністратору. Цей канал комунікації забезпечує миттєве отримання сповіщень про підозрілі активності незалежно від географічної позиції фахівця.

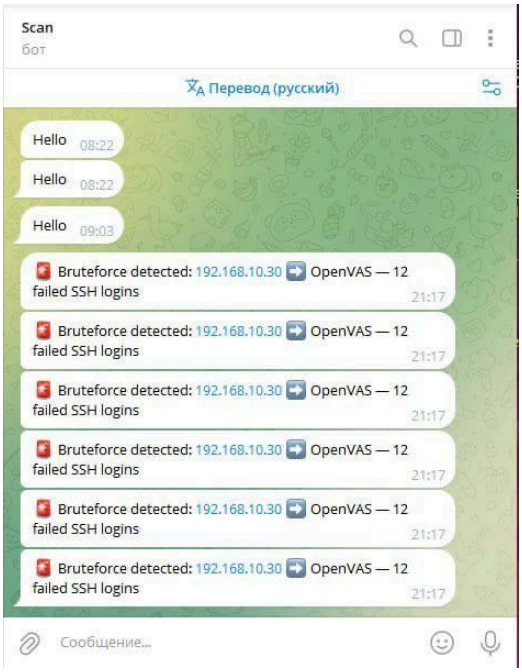

Рис. 4.9. Сповіщення у Telegram, що забезпечило оперативність реагування

ВИСНОВКИ ДО РОЗДІЛУ 4

Узагальнений аналіз довів, що інтеграція систем керування подіями безпеки з підсистемами виявлення та запобігання вторгнень формує цілісний контур моніторингу, здатний забезпечити своєчасне виявлення складних багатоступеневих загроз і зниження операційного ризику для критично важливих сервісів. Об’єднання потоків журналів від операційних систем, мережевих пристроїв, засобів захисту кінцевих точок, прикладних компонентів та датчиків IDS/IPS у єдиному сховищі зі

стандартизованою нормалізацією даних створює основу для надійної кореляції подій. За рахунок цього ізольовані сигнали — невдалі спроби автентифікації, нетипові мережеві з’єднання, модифікації прав доступу, поведінкові аномалії — набувають змісту у вигляді підтвердженої часової послідовності, що віддзеркалює реальну траєкторію атаки від розвідки та експлуатації вразливості до закріплення і можливого виведення даних.

Додаткове впровадження систематичного сканування вразливостей із пріоритизацією за критичністю активів і наслідками для бізнес-процесів забезпечує превентивний вплив на поверхню атаки. Регулярний цикл виявлення та усунення відомих недоліків конфігурації і програмного забезпечення суттєво зменшує ймовірність успішної експлуатації та скорочує час, протягом якого вразливості залишаються придатними для використання зловмисниками. У поєднанні з кореляційними правилами подій та поведінковими індикаторами такий превентивний блок підсилює здатність системи до раннього попередження та локалізації інцидентів.

Практична придатність підходу підтверджується можливістю побудови прозорої ситуаційної картини на аналітичних панелях, орієнтованих на задачі оперативного центру безпеки: візуалізація динаміки атак і джерел загроз, контроль найкритичніших подій автентифікації та доступу, моніторинг ефективності засобів захисту кінцевих точок і мережевих екрануючих політик. Такі панелі, разом із налаштованими механізмами оповіщення, скорочують середній час виявлення та реагування, уможливлюють пріоритизацію ресурсів за ступенем впливу на цілісність, конфіденційність і доступність інформації.

Окремим результатом є формування відтворюваного процесу реагування на інциденти, узгодженого з кращими практиками управління: від первинного тріажу та побудови таймлайна з мапуванням на MITRE ATT&CK до стримування, ліквідації, керованого відновлення та аналізу уроків. Забезпечення доказовості — синхронізація часу, контроль цілісності журналів і артефактів, прозорий ланцюг зберігання — підвищує довіру до результатів розслідування та дозволяє використовувати їх у подальшому управлінні ризиками. Наявність узгоджених шаблонів реєстрації,

таксономій і метрик якості (у тому числі MTTD та MTTR) створює підґрунтя для постійного вдосконалення процесів та вимірюваного підвищення кіберстійкості.

Комплексний підхід, що поєднує централізоване журналювання, кореляцію подій, превентивне сканування вразливостей і стандартизований цикл реагування, є технологічно і методично доцільним для захисту об’єктів, критичних з точки зору безперервності державних і суспільно значущих послуг. Його масштабування передбачає нарощування покриття джерел телеметрії, інтеграцію з платформами оркестрації та автоматизації реагування, розширення використання розвідки загроз і впровадження поведінкової аналітики для фіксації аномалій, зокрема у випадках атак нульового дня. Водночас зберігається вимога до системної роботи з людським фактором: підготовка персоналу, регулярні навчання та перевірки, чіткі регламенти ескалації та комунікацій під час інцидентів.

Сукупний ефект від реалізованого рішення полягає у підвищенні якості моніторингу, скороченні часу до виявлення та усунення загроз, покращенні оглядовості ризиків і підзвітності управлінських рішень. За рахунок цього знижується ймовірність матеріальних і репутаційних втрат, а також забезпечується відповідність вимогам нормативно-правових актів і стандартів у сфері інформаційної безпеки. Отримані результати свідчать про доцільність подальшого розгортання та уніфікації зазначених практик у масштабі розподілених середовищ, з особливим акцентом на об’єктах критичної інформаційної інфраструктури, де неперервність функціонування безпосередньо пов’язана з національною безпекою та громадською безпекою.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ

Питання охорони праці людини є критично важливим при розробці методів та моделей управління кіберінцидентами в організаціях та на підприємствах критичної інфраструктури. Забезпечення безпечних і здорових умов праці спеціалістів, які займаються аналізом, реагуванням та запобіганням кіберінцидентам, значною мірою залежить від правильної оцінки небезпечних і шкідливих виробничих факторів, які супроводжують їхню професійну діяльність.

Спеціалісти з управління кіберінцидентами, як правило, працюють у напруженому середовищі з використанням персональних комп'ютерів, серверів та іншого обладнання, що створює комплекс факторів, здатних негативно впливати на їхнє здоров'я та працездатність. Розумова праця фахівців характеризується великим нервово-емоційним напруженням, інтенсивною розумовою активністю, необхідністю постійної концентрації уваги та швидкої прийняття рішень в умовах дефіциту часу. При інтенсивній інтелектуальній роботі мозок споживає від 15 до 20 відсотків від загального обсягу енергії організму, а вживання кисню корою головного мозку в п'ять разів перевищує споживання кисню скелетними м'язами при максимальному фізичному навантаженні.

5.1. Характеристика умов праці фахівців центру управління кіберінцидентами

Центр управління кіберінцидентами (далі - ЦУКІ) критичної інфраструктури розташовується в спеціально обладнаному приміщенні з підвищеними вимогами до безпеки та надійності. Приміщення ЦУКІ має наступні характеристики: довжина 12 метрів, ширина 8 метрів, загальна площа 96 квадратних метрів, висота стелі 3,5 метра. У приміщенні розташовано 10 робочих місць операторів-аналітиків з управління кіберінцидентами, кожне з яких обладнане робочим столом площею 1,8 квадратних

метра, ергономічним кріслом та персональним комп'ютером із двома моніторами діагоналлю 24 дюйми.

Відповідно до Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98, площа на одне робоче місце має становити не менше ніж 6,0 квадратних метрів, а об'єм не менше ніж 20,0 кубічних метрів. Розрахуємо відповідність приміщення встановленим нормам:

- Площа на одне робоче місце: $S = 96 м^2 / 10 = 9,6 м^2$ (норма $\geq 6,0 м^2$) - відповідає нормі

- Об'єм на одне робоче місце: $V = (96 м^2 \times 3,5 м) / 10 = 33,6 м^3$ (норма $\geq 20,0 м^3$) - відповідає нормі

Робочі місця розташовані таким чином, щоб між бічними поверхнями моніторів була відстань не менше 1,2 метра, а від тильної поверхні одного монітора до екрана іншого - не менше 2,5 метра. Екрани моніторів розташовані на оптимальній відстані від очей користувача, що становить 600-700 міліметрів, з урахуванням розміру літерно-цифрових знаків і символів. Розташування екрану забезпечує зручність зорового спостереження у вертикальній площині під кутом плюс-мінус 30 градусів до нормальної лінії погляду працюючого.

Робота фахівців з управління кіберінцидентами відноситься до категорії легких робіт (категорія Іа-Іб за класифікацією фізичних робіт), оскільки вона переважно розумова, з незначним фізичним навантаженням, виконується в позі сидячи у стабільних умовах. За характером трудової діяльності персонал ЦУКІ можна класифікувати наступним чином:

Група 1. Аналітики кіберзагроз - виконують роботу з аналізу даних про кіберзагрози з використанням спеціалізованого програмного забезпечення. Робота характеризується інтенсивною розумовою творчою працею з підвищеним напруженням зору, концентрацією уваги на фоні нервово-емоційного напруження, вимушеною робочою позою, загальною гіподинамією. Робота виконується в режимі постійного моніторингу інформаційних потоків.

Група 2. Оператори систем виявлення інцидентів - здійснюють облік інформації про кіберінциденти, що надходить з систем моніторингу, супроводжується перервами різної тривалості та характеризується напруженням зору, невеликими фізичними зусиллями, нервовим напруженням середнього ступеня.

Група 3. Фахівці з реагування на інциденти - виконують роботи з локалізації та усунення наслідків кіберінцидентів, що вимагає швидкого прийняття рішень в умовах обмеженого часу, високого рівня концентрації уваги та стресостійкості.

5.2. Мікроклімат робочої зони та його нормалізація

Мікроклімат робочої зони є одним з ключових параметрів, які впливають на здоров'я та продуктивність спеціалістів з управління кіберінцідентами. Мікроклімат - це комплекс фізичних параметрів повітря, що включає температуру, відносну вологість, швидкість руху повітря та інтенсивність теплового випромінювання.

Для робіт категорії Іа-Іб відповідно до ДСанПіН 3.3.6.042-99 "Санітарні норми мікроклімату виробничих приміщень" встановлено наступні оптимальні параметри мікроклімату:

Холодний період року (середня температура зовнішнього повітря нижче +10°С):

- Температура повітря: 22-24°С
- Відносна вологість: 60-40%
- Швидкість руху повітря: не більше 0,1 м/с

Теплий період року (середня температура зовнішнього повітря +10°С і вище):

- Температура повітря: 23-25°С
- Відносна вологість: 60-40%
- Швидкість руху повітря: не більше 0,2 м/с

У приміщенні ЦУКІ розташована значна кількість електронно-обчислювальної техніки (10 персональних комп'ютерів із 20 моніторами, 2 сервери, комутаційне обладнання, системи відеоспостереження), яка є джерелом тепловиділень. Крім того,

джерелами інфрачервоного випромінювання є нагріті поверхні опалювальної системи в холодний період року.

Для підтримання оптимальних параметрів мікроклімату необхідно розрахувати необхідний повітрообмін. Розрахунок виконується за надлишками явного тепла, що виділяється в приміщенні.

Визначення тепловиділень від обладнання:

Теплові виділення від одного комп'ютера з монітором складають приблизно 250 Вт. У приміщенні розташовано 10 комп'ютерів з 20 моніторами, тому:

$$Q_1 = 10 \times 250 \text{ Вт} = 2500 \text{ Вт} = 2{,}5 \text{ кВт}, \quad (5.1)$$

Теплові виділення від серверного обладнання (2 сервери):

$$Q_2 = 2 \times 400 \text{ Вт} = 800 \text{ Вт} = 0{,}8 \text{ кВт}, \quad (5.2)$$

Теплові виділення від комутаційного обладнання та систем відеоспостереження:

$$Q_3 = 300 \text{ Вт} = 0{,}3 \text{ кВт}, \quad (5.3)$$

Теплові виділення від людей (10 осіб при легкій роботі - 100 Вт на людину):

$$Q_4 = 10 \times 100 \text{ Вт} = 1000 \text{ Вт} = 1{,}0 \text{ кВт}, \quad (5.4)$$

Загальні тепловиділення:

$$Q\_заг = Q_1 + Q_2 + Q_3 + Q_4 = 2{,}5 + 0{,}8 + 0{,}3 + 1{,}0 = 4{,}6 \text{ кВт} = 4600 \text{ Вт}, \quad (5.5)$$

Розрахунок необхідного повітрообміну:

Необхідний повітрообмін L (м³/год) визначається за формулою:

$$L = Q\_заг / (c \times \rho \times \Delta t) , \quad (5.6)$$

де:

- Q_заг - надлишки явного тепла, Вт (4600 Вт)
- c - питома теплоємність повітря, 1005 Дж/(кг·°С)
- ρ - густина повітря, 1,2 кг/м³
- Δt - різниця температур між повітрям, що видаляється та припливним повітрям, °С (приймаємо 5°С)

$$L = 4600 / (1005 \times 1,2 \times 5) = 4600 / 6030 = 0,763 \text{ м}^3/\text{с} = 2747 \text{ м}^3/\text{год}, \quad (5.7)$$

Для забезпечення нормального мікроклімату необхідно забезпечити повітрообмін не менше 2750 м³/год або 46 м³/хв.

Кратність повітрообміну:

$$n = L / V\_прим = 2747 / (96 \times 3,5) = 2747 / 336 = 8,2 \text{ обмінів/год}, \quad (5.8)$$

Отримана кратність повітрообміну відповідає санітарним нормам для приміщень з комп'ютерною технікою (рекомендована кратність 5-10 обмінів/год).

Для забезпечення оптимальних параметрів мікроклімату в приміщенні ЦУКІ необхідно застосовувати систему кондиціонування повітря з автоматичним підтримуванням заданих параметрів температури та вологості. У холодний період року використовується водяне опалення з терморегуляторами, що дозволяє підтримувати температуру в межах 22-24°С [25].

Система вентиляції повинна забезпечувати як загальнообмінну, так і місцеву вентиляцію в зонах інтенсивного тепловиділення (серверне обладнання). Для контролю параметрів мікроклімату необхідно встановити датчики температури та вологості з виведенням інформації на пульт оператора системи життєзабезпечення.

5.3. Освітлення робочих місць та його розрахунок

Якість освітлення робочого місця має надзвичайно важливе значення для здоров'я та продуктивності спеціалістів, які працюють з персональними комп'ютерами. Робота операторів ЦУКІ відноситься до робіт середньої точності (четвертий розряд зорових робіт відповідно до ДБН В.2.5-28-2006 "Природне і штучне освітлення"), оскільки мінімальний розмір об'єкту розрізнення на екрані монітора складає від 0,5 до 1,0 міліметра.

Нормовані параметри природного освітлення:

Коефіцієнт природного освітлення (КПО) для приміщень з роботами четвертого розряду при бічному освітленні повинен становити не менше 1,5%. КПО - це відношення освітленості в середині приміщення до освітленості тієї ж поверхні відкритим небосхилом, виражене у відсотках.

Нормовані параметри штучного освітлення:

- Мінімальна освітленість (E_мін) для робіт четвертого розряду: 300-500 лк
- Коефіцієнт пульсації світлового потоку (K_п): не більше 20%
- Показник дискомфорту (M): не більше 40
- Коефіцієнт природної освітленості вертикальної поверхні екрану монітора: не більше 200 лк

Для розрахунку необхідної кількості світильників використовуємо метод коефіцієнта використання світлового потоку.

- Вихідні дані:
- Площа приміщення: S = 96 м²
- Ширина приміщення: A = 8 м
- Довжина приміщення: B = 12 м
- Висота приміщення: H = 3,5 м
- Висота робочої поверхні: h_p = 0,8 м
- Висота світильників над підлогою: h_c = 3,2 м
- Нормована освітленість: E = 400 лк
- Коефіцієнт запасу: K = 1,5 (для приміщень з комп'ютерною технікою)

- Коефіцієнт нерівномірності освітлення: Z = 1,1
- Коефіцієнт відбиття стелі: ρ_стелі = 70%
- Коефіцієнт відбиття стін: ρ_стін = 50%
- Коефіцієнт відбиття підлоги: ρ_підлоги = 30%

Крок 1. Визначення розрахункової висоти підвісу світильників:

$$h = h_c - h_p = 3,2 - 0,8 = 2,4 \text{ м}, \quad (5.9)$$

Крок 2. Розрахунок індексу приміщення:

$$i=(A\times B)/[h\times(A+B)]=(8\times12)/[2,4 \times (8 +12)]=96/(2,4\times20=96/48=2,0, \quad (5.10)$$

Крок 3. Визначення коефіцієнта використання світлового потоку:

За таблицями для світильників типу ЛПО з люмінесцентними лампами або світлодіодними лампами, при індексі приміщення i = 2,0 та коефіцієнтах відбиття ρ_стелі = 70%, ρ_стін = 50%, коефіцієнт використання світлового потоку η = 0,52.

Крок 4. Розрахунок необхідного світлового потоку:

$$F=(E\times S\times K\times Z)/\eta=(400\times96\times1,5\times1,1)/0,52 = 63\ 360 / 0,52 = 121\ 846 \text{ лм}, \quad (5.11)$$

Крок 5. Вибір типу світильників та ламп:

Для забезпечення якісного освітлення вибираємо світлодіодні панелі типу LED-панель 600×600 мм з світловим потоком одної панелі F_л = 4500 лм (потужність 40 Вт, колірна температура 4000К - нейтральний білий, коефіцієнт пульсації < 5%).

Крок 6. Розрахунок необхідної кількості світильників:

$$N = F / F_л = 121\ 846 / 4500 = 27,1 \approx 28 \text{ світильників}, \quad (5.12)$$

Крок 7. Розміщення світильників:

Оптимальне розміщення - у вигляді прямокутної сітки 4 ряди × 7 світильників = 28 світильників. Відстань між рядами світильників: $L_1 = 12 / 4 = 3,0$ м. Відстань між світильниками в ряду: $L_2 = 8 / 7 \approx 1,14$ м.

Перевірка розрахунку:

Фактична освітленість:

$$E\_факт = (N \times F\_л \times \eta) / (S \times K \times Z) = (28 \times 4500 \times 0,52) / (96 \times 1,5 \times 1,1) = 65$$

$$520 / 158,4 = 413,6 \text{ лк}, \quad (5.13)$$

Отримане значення E_факт = 413,6 лк знаходиться в межах нормованого діапазону 300-500 лк, що підтверджує правильність розрахунку [25].

Для підтримки запроектованого рівня освітлення необхідно:

1. Проводити очищення світильників та віконних блоків не менше 2 разів на рік
2. Своєчасно замінювати вихідні з ладу лампи
3. Розташовувати робочі місця таким чином, щоб природне світло падало збоку, переважно зліва
4. Використовувати на вікнах регульовані жалюзі для контролю інтенсивності природного освітлення
5. Уникати розташування моніторів навпроти вікон або яскравих джерел світла
6. При необхідності використовувати антибликові фільтри на моніторах

5.4. Електромагнітне випромінювання та електробезпека

Електромагнітне випромінювання (ЕМВ) є одним з найбільш серйозних чинників виробничого середовища при роботі з комп'ютерною технікою. Джерелами ЕМВ в приміщенні ЦУКІ є:

- Монітори персональних комп'ютерів (20 моніторів)
- Системні блоки комп'ютерів (10 шт.)

- Серверне обладнання (2 сервери)
- Мережеве комутаційне обладнання (маршрутизатори, комутатори)
- Системи безперебійного живлення (UPS)
- Кабельні лінії електроживлення та передачі даних

Відповідно до Державних санітарних правіл і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98, встановлено наступні допустимі значення параметрів неіонізуючих електромагнітних випромінювань:

Діапазон частот 5 Гц - 2 кГц:

- Напруженість електричної складової: E ≤ 25 В/м
- Напруженість магнітної складової: H ≤ 250 нТл (0,25 А/м)

Діапазон частот 2 кГц - 400 кГц:

- Напруженість електричної складової: E ≤ 2,5 В/м
- Напруженість магнітної складової: H ≤ 25 нТл (0,025 А/м)

Електростатичне поле:

- Напруженість електростатичного поля: E ≤ 20 кВ/м

Рентгенівське випромінювання:

- Потужність експозиційної дози на відстані 0,05 м від поверхні екрана: ≤ 100 мкР/год (1 мкЗв/год)

Для визначення безпечної відстані від екрану монітора використовуємо формулу:

$r = \sqrt{(P \times G / (4\pi \times П\_доп))}$

де:

- P - потужність випромінювання джерела, Вт
- G - коефіцієнт посилення антени (для монітора G ≈ 1)
- П_доп - допустима щільність потоку енергії, Вт/м²
- r - безпечна відстань, м

Для монітора з діагоналлю 24 дюйми потужність ЕМВ у діапазоні високих частот складає приблизно P = 0,1 Вт, допустима щільність потоку енергії П_доп = 10 Вт/м².

$$r = \sqrt{(0,1 \times 1 / (4 \times 3,14 \times 10))} = \sqrt{(0,1 / 125,6)} = \sqrt{0,000796} = 0,028 \text{ м} = 2,8 \text{ см}, \quad (5.14)$$

Однак для зручності роботи та запобігання утомі очей рекомендована відстань від очей до екрану становить 600-700 мм, що значно перевищує розраховану безпечну відстань за критерієм ЕМВ.

Для мінімізації впливу ЕМВ на здоров'я фахівців ЦУКІ рекомендується:

1. Технічні заходи:

- Використання моніторів з низьким рівнем випромінювання (стандарти TCO, MPR II)
- Застосування екранованих кабелів для з'єднання обладнання
- Розташування серверного обладнання в окремому технічному приміщенні
- Заземлення всього електронного обладнання

2. Організаційні заходи:

- Розташування робочих місць на відстані не менше 1,2 м між моніторами
- Відстань від тильної поверхні монітора до наступного робочого місця не менше 2,5 м
- Періодичні перерви в роботі з комп'ютером
- Регулярний контроль рівнів ЕМВ

3. Індивідуальні засоби захисту:

- Використання спеціальних окулярів з захисним покриттям
- Застосування антистатичних килимків
- Підтримка відносної вологості повітря 40-60% для зменшення статичної електрики

Приміщення ЦУКІ за ступенем небезпеки ураження електричним струмом відноситься до класу приміщень без підвищеної небезпеки (відповідно до Правил улаштування електроустановок - ПУЕ), оскільки є сухим приміщенням з нормальною температурою повітря та ізольованою підлогою [25].

Основні заходи електробезпеки:

- Заземлення металевих корпусів електрообладнання

- Застосування УЗО (пристроїв захисного відключення)
- Використання подвійної ізоляції
- Регулярний інструктаж персоналу з електробезпеки

Розрахунок заземлюючого пристрою:

Для забезпечення електробезпеки необхідно розрахувати заземлюючий пристрій. Відповідно до ПУЕ, для електроустановок напругою до 1000 В опір заземлюючого пристрою не повинен перевищувати 4 Ом.

Використовуємо вертикальні заземлювачі - сталеві труби діаметром d = 50 мм, довжиною l = 2,5 м, заглиблені в грунт на глибину t = 0,8 м. Грунт - суглинок з питомим опором ρ = 100 Ом·м.

Опір розтіканню струму одного вертикального заземлювача:

$$R\_верт = (\rho / 2\pi l) \times [\ln(2l/d) + 0,5 \times \ln((4t + l)/(4t - l))] , \quad (5.15)$$

$$R\_верт=(100/(2\times3,14\times2,5))[\ln(2\times2,5/0,05)+0,5\times\ln((4\times0,8+2,5)/(4\times0,8-2,5))], \quad (5.16)$$

$$R\_верт = (100 / 15,7) \times [\ln(100) + 0,5 \times \ln(5,7/0,7)] , \quad (5.17)$$

$$R\_верт=6,37\times[4,605+0,5\times2,098]=6,37\times[4,605+1,049]=6,37\times5,654=36 \text{ Ом}, \quad (5.18)$$

Необхідна кількість вертикальних заземлювачів:

З урахуванням коефіцієнта використання заземлювачів η_в = 0,6 (для групи з 4-6 заземлювачів, розташованих у ряд з відстанню між ними 2,5 м):

$$n = R\_верт / (R\_норм \times \eta\_в) = 36 / (4 \times 0,6) = 36 / 2,4 = 15, \quad (5.19)$$

Приймаємо n = 16 вертикальних заземлювачів, з'єднаних горизонтальною сталевою смугою 40×4 мм.

5.5. Особливості охорони праці в умовах кризових ситуацій

Управління кіберінцидентами в організаціях критичної інфраструктури вимагає особливої уваги до охорони праці персоналу в умовах кризових ситуацій. Кризова ситуація у сфері кібербезпеки - це надзвичайна подія, пов'язана з кіберінцидентом, кібератакою або кіберзагрозою, яка створює загрозу безпеці критичної інфраструктури та вимагає скоординованого реагування на національному рівні.

Відповідно до Національного плану реагування на кіберінциденти, затвердженого постановою Кабінету Міністрів України, при виникненні кризової ситуації активізується Національна система реагування на кіберінциденти, до якої входять CERT-UA (національна команда реагування на кіберінциденти) та галузеві/регіональні команди реагування [26].

У період кризових ситуацій, пов'язаних з масштабними кібератаками на об'єкти критичної інфраструктури, фахівці ЦУКІ піддаються впливу додаткових небезпечних та шкідливих факторів:

1. Підвищене нервово-психологічне навантаження:
- Необхідність прийняття швидких рішень в умовах невизначеності
- Робота в умовах дефіциту часу та підвищеної відповідальності
- Можливість виникнення паніки та стресових станів
- Порушення звичного режиму праці та відпочинку

2. Тривала безперервна робота за комп'ютером:
- Збільшення часу роботи з 8 до 12-16 годин на добу
- Скорочення або відсутність регламентованих перерв
- Підвищена втома очей та опорно-рухового апарату
- Накопичення фізіологічного стомлення

3. Робота в режимі цілодобового чергування:
- Порушення природних біоритмів організму при нічних змінах
- Зниження концентрації уваги в нічний час
- Підвищений ризик помилок через втому
- Проблеми з організацією харчування та відпочинку

4. Підвищене електромагнітне навантаження:

- Збільшення часу експозиції до ЕМВ через тривалу роботу
- Одночасне використання кількох моніторів
- Інтенсивне використання засобів зв'язку (мобільні телефони, рації)

Для забезпечення ефективної роботи та збереження здоров'я персоналу в умовах кризової ситуації необхідно впровадити наступні організаційні заходи:

1. Режим праці та відпочинку:

При переході в режим кризового реагування встановлюється посилений режим роботи з наступними параметрами:

- Тривалість робочої зміни: не більше 12 годин
- Організація роботи за графіком: 2 зміни по 12 годин або 3 зміни по 8 годин
- Обов'язкові регламентовані перерви:
- Перша година роботи: 10 хвилин після 50 хвилин роботи
- Кожні наступні 2 години: 15 хвилин після 105 хвилин роботи
- Обідня перерва: 45 хвилин після 4 годин роботи

2. Організація кімнати психологічного розвантаження:

У приміщенні, суміжному з ЦУКІ, обладнується спеціальна кімната психологічного розвантаження площею не менше 24 м² (з розрахунку 2 м² на одну особу при одночасному перебуванні 12 осіб - змінного складу).

Кімната обладнується:

- М'якими меблями для відпочинку (крісла-реклайнери, диван)
- Системою регульованого освітлення з можливістю створення приглушеного світла
- Аудіосистемою для відтворення релаксаційної музики
- Апаратом для приготування гарячих напоїв
- Системою ароматерапії з заспокійливими ароматами

3. Медичне забезпечення:

- Наявність аптечки першої допомоги з препаратами для зняття стресу
- Можливість оперативної консультації з лікарем (телемедицина)

- Профілактичний прийом вітамінів групи В та адаптогенів
- Контроль артеріального тиску та пульсу персоналу перед зміною та після неї

4. Ергономічна організація робочих місць:

В умовах тривалої роботи особливо важливо забезпечити ергономічну організацію робочих місць:

- Використання ергономічних крісел з можливістю регулювання всіх параметрів
- Застосування підставок для ніг (висота 100-150 мм, кут нахилу 10-20°)
- Використання окремих клавіатур та мишок з ергономічним дизайном
- Забезпечення підставок для документів, розташованих на рівні екрану монітора
- Можливість роботи стоячи (висувні столи з регульованою висотою)

Для зменшення негативного впливу тривалої роботи за комп'ютером рекомендується виконувати комплекси спеціальних вправ:

Вправи для очей (виконуються кожні 40-50 хвилин):

- Заплющити очі та інтенсивно покліпати 10-15 разів
- "Намалювати" очима вісімку (вертикальну та горизонтальну) по 5 разів
- Фіксувати погляд на найвіддаленішій точці (5 секунд), потім на кінчику носа (5 секунд) - повторити 10 разів
- Круговий рух очима за годинниковою стрілкою та проти (по 10 разів)
- Масаж скронь біля кутиків очей круговими рухами (1 хвилина)

Вправи для шийного відділу хребта (виконуються кожні 2 години):

- Повільні нахили голови вперед-назад (10 разів)
- Повільні нахили голови вліво-вправо (10 разів)
- Повільні повороти голови вліво-вправо (10 разів)
- Кругові обертання головою (по 5 разів у кожен бік)
- Підняття та опускання плечей (15 разів)

Вправи для кистей рук (виконуються кожну годину):

- Стискання та розтискання кулаків (20 разів)

- Обертання кистями за годинниковою стрілкою та проти (по 10 разів)
- "Струшування" кистей рук (30 секунд)
- Розтягування пальців з опором (кожен палець по 5 секунд)

Робота в умовах кризової ситуації супроводжується підвищеним стресом, тому необхідно забезпечити психологічну підтримку персоналу:

Психологічна підготовка:

- Проведення тренінгів з управління стресом
- Формування психологічної стійкості через симуляційні вправи

Психологічний супровід під час кризи:

- Можливість консультації з психологом у будь-який час
- Групові сеанси психологічного розвантаження після зміни
- Індивідуальна робота з працівниками, які демонструють ознаки перенапруження

Посткризова реабілітація:

- Обов'язкова консультація з психологом після завершення кризи
- Надання додаткових днів відпочинку (не менше 3 днів після 7-денної роботи в кризовому режимі)
- Моніторинг психологічного стану протягом місяця після кризових ситуацій

У приміщенні ЦУКІ повинен бути розроблений та затверджений план евакуації на випадок виникнення надзвичайних ситуацій (пожежа, витік небезпечних речовин, тероризм тощо). План евакуації повинен містити:

- Схему евакуаційних шляхів та виходів
- Місце розташування первинних засобів пожежогасіння
- Місце розташування аптечки першої допомоги
- Номери телефонів екстрених служб
- Прізвища відповідальних осіб за евакуацію
- Персонал ЦУКІ повинен пройти навчання та практичні тренування з евакуації не рідше 2 разів на рік.

ВИСНОВКИ ДО РОЗДІЛУ 5

Охорона праці фахівців центру управління кіберінцидентами у критичній інфраструктурі є комплексною задачею, яка вимагає постійної уваги до умов праці та факторів виробничого середовища. Основними напрямками забезпечення безпечних умов праці є:

Нормалізація мікроклімату - підтримання оптимальних параметрів температури (22-25°С), вологості (40-60%) та повітрообміну (не менше 2750 м³/год для приміщення площею 96 м²) за допомогою систем вентиляції та кондиціонування.

Забезпечення належного освітлення - створення комбінованого освітлення з мінімальним рівнем 400 лк за рахунок встановлення 28 світлодіодних світильників з коефіцієнтом пульсації менше 5%.

Мінімізація впливу електромагнітного випромінювання - використання сертифікованого обладнання з низьким рівнем ЕМВ, правильне розташування робочих місць, заземлення обладнання та дотримання безпечних відстаней.

Особливі заходи в умовах кризових ситуацій - організація раціонального режиму праці та відпочинку при тривалих змінах, створення умов для психологічного розвантаження, медичне забезпечення та психологічна підтримка персоналу.

Впровадження розроблених заходів дозволить забезпечити безпечні умови праці, зберегти здоров'я та працездатність фахівців ЦУКІ, підвищити ефективність їх роботи при управлінні кіберінцидентами в організаціях та на підприємствах критичної інфраструктури.

РОЗДІЛ 6
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

Розвиток інформаційних технологій та розширення використання цифрових систем у критичній інфраструктурі супроводжується зростанням негативного впливу на навколишнє природне середовище. Техногенне середовище (техносфера), як складова навколишнього середовища, є похідною від діяльності людини і виникла як наслідок впливу антропогенних чинників. На сьогоднішній день практично все середовище, в якому перебуває людина, має ознаки техногенного впливу.

При управлінні кіберінцидентами в організаціях та на підприємствах критичної інфраструктури необхідно розглядати як прямий вплив на довкілля через техногенні фактори, так і непрямі наслідки цієї діяльності [25].

Людина, діючи у техногенному середовищі, безперервно виконує два основних завдання:

1. Забезпечує своє комфортне перебування у середовищі проживання та праці
2. Створює та використовує системи захисту від впливу його негативних чинників

6.1. Аналіз впливу техногенних чинників на навколишнє середовище

Розрізняють прямий і непрямий вплив на навколишнє середовище та організм людини негативних чинників техносфери.

Прямий вплив:

- Безпосередні викиди та скиди забруднюючих речовин
- Вибухи та вибухи енергії
- Явні утворення відходів

Непрямий вплив:

- Опосередковане забруднення через ланцюги харчування
- Накопичення токсичних речовин в організмі
- Алергічні реакції на забруднювачі

При функціонуванні систем управління кіберінцидентами та захисту критичної інфраструктури основні техногенні фактори, що впливають на навколишнє середовище, включають:

Енергетичне навантаження та теплові викиди:

- Споживання електроенергії серверами, комп'ютерами та мережевим обладнанням

- Теплові викиди від охолоджуючих систем центрів обробки даних

- Опалювальні та кондиціонувальні системи приміщень

Один персональний комп'ютер споживає 150-300 Вт електроенергії, а при постійній роботі 100 комп'ютерів це становить 15-30 кВт. На більших операціях управління кіберінцидентами з десятками та сотнями комп'ютерів енергоспоживання досягає мегаватних величин.

Електромагнітні поля:

- Випромінювання від радіоелектронних засобів та комунікаційного обладнання

- Лінії електропередач та розподільні мережі

- Мобільні та бездротові системи комунікації, необхідні для забезпечення безперервності операцій

- Системи супутникового зв'язку та GPS

Забруднення атмосфери:

- Викиди від енергогенеруючих установок (у разі відмов основного енергопостачання, генератори спалюють дизельне паливо)

- Повітряні забруднення від систем вентиляції, які видаляють гарячий та забруднений повітря

- Пари хімічних речовин від систем охолодження

Електронні відходи та забруднення грунту:

- Утилізація застарілого комп'ютерного обладнання, яке містить токсичні речовини

- Вихід з ладу приладів та елементів живлення (батарейки, конденсатори)

- Накопичення матеріалів, які містять свинець, ртуть, кадмій та інші важкі метали

- Неправильна утилізація пластику та інших синтетичних матеріалів

Принцип дії ЕМП на організм людини:

Електромагнітне поле впливає на заряджені частинки і електричні струми в живих організмах, внаслідок чого енергія поля на рівні клітини перетворюється в інші види енергії (теплову, хімічну, механічну).

Вплив на клітинний рівень:

Цитогенетичні дослідження (вихід хромосомних аберацій) показали достовірне збільшення клітин з порушеннями в експериментальній групі порівняно з контролем. Збільшення хромосомних аберацій було також виявлено при опроміненні ЕМП живих організмів та рослинного матеріалу. Цитогенетичний аналіз клітин крові показав підвищену кількість генетичних ушкоджень.

Вплив на тканини:

Слабкі електромагнітні поля при інтенсивності менше порогу теплового ефекту також впливають на зміни в живій тканині. Атоми і молекули в електричному полі поляризуються, полярні молекули орієнтуються у напрямку розповсюдження магнітного поля. Змінне електричне поле викликає нагрівання тканин живих організмів як за рахунок змінної поляризації діелектрика (сухожиль, хрящів, кісток), так і за рахунок появи струмів провідності.

Вплив на нервову систему:

Експериментальні дослідження встановили наявність прямої дії ЕМП на мозок, мембрани нейронів, пам'ять, умовно-рефлекторну діяльність. У модельних експериментах показана можливість впливу слабких ЕМП на процеси синтезу в нервових клітинах. Отримано виразні зміни імпульсації коркових нейронів, що призводять до порушення переданої інформації в більш складні структури мозку. Виявлено, що при дії ЕМП у надвисокочастотному діапазоні може розвинутися порушення короткочасної пам'яті.

Вплив на імунну систему:

При дії ЕМП порушуються процеси імуногенезу. Встановлено, що під впливом ЕМП змінюється характер інфекційного процесу, виникають порушення білкового обміну, спостерігається зниження вмісту альбумінів і підвищення гамма-глобулінів в крові. Крім того, ЕМП може виступати в якості алергену або пускового фактора, викликаючи важкі реакції у хворих алергіків.

Вплив на репродуктивну систему:

Під впливом ЕМП знижується функція сперматогенезу у чоловіків, змінюється менструальний цикл у жінок, уповільнюється ембріональний розвиток плода, виникають вроджені аномалії в новонароджених дітей і зменшується лактація у годуючих матерів.

Вплив на рослини:

Численні дослідження показали, що ЕМ хвилі істотно впливають на біологічні об'єкти. Як слабкі, так і сильні ЕМП надають виражений вплив на морфологічні, фізіологічні, біохімічні та біофізичні характеристики багатьох рослин. Вони впливають на зростання, розвиток і розмноження рослинних об'єктів. Спостереження показали зменшення сухої ваги надземної маси рослин, що зростають під ПЛ, у порівнянні з контролем. Виявлено негативний вплив ЕМП на потенційну нітрогенезну активність грунтової популяції, довжину проростків рослин [27].

Загальний вплив слабких ЕМП на живі організми:

Результати досліджень біологічного впливу радіоелектронних засобів виявилися такими:

- Зниження рухової активності і виживання мікроорганізмів
- Збільшення смертності мікроорганізмів та інших біологічних об'єктів
- Погіршення регенерації тканин
- Порушення ембріонального і личинкового розвитку
- Зниження біохімічних реакцій, порушення метаболізму
- Зниження енергетичного потенціалу у всіх життєво важливих системах організму

6.2. Методи та засоби захисту навколишнього середовища від впливу техногенних чинників

Для мінімізації впливу ЕМВ на персонал, населення та екосистеми, які знаходяться у зоні дії радіоелектронних засобів, необхідно вжити комплекс організаційних, інженерно-технічних та лікарсько-профілактичних заходів.

Організаційні заходи:

- Розробка та впровадження політики щодо охорони навколишнього середовища на рівні організації

- Оцінка впливу планованої діяльності на довкілля на стадії проектування систем управління кіберінцидентами

- Регулярний моніторинг та контроль рівнів електромагнітного поля у приміщеннях та навколо них

- Отримання дозволів та узгодження з органами санітарного нагляду перед встановленням нового обладнання

- Регулярні перевірки дотримання гігієнічних норм спеціалізованими лабораторіями

Інженерно-технічні методи:

Колективний захист (масштаб територій):

- Розрахунок поширення радіохвиль в умовах конкретного рельєфу місцевості на стадії проектування

- Оптимальне взаємне розташування опромінюючих та опромінюваних об'єктів з мінімізацією інтенсивності опромінення

- Використання природних екранів (складки місцевості, лісонасадження, нежитлові будівлі)

- Розташування антен на висоті, що забезпечує зменшення інтенсивності поля на території населених пунктів у кілька разів

- Оптимізація діаграми спрямованості антен, особливо високоспрямованих, шляхом збільшення висоти антени

Локальний захист (окремі приміщення):

- Екранування приміщень радіозахисними матеріалами (металеві листи та сітки з доброю провідністю)

- Обклеювання стін металізованими шпалерами, що мають високе поглинання енергії випромінювання

- Захист вікон сітками та металізованими шторами

- Встановлення антиблікових та радіозахисних фільтрів на монітори комп'ютерів

- Використання радіопоглинальних матеріалів у конструкціях приміщень

Індивідуальний захист (засоби захисту персоналу):

- Спеціальний одяг із металізованих тканин та радіопоглинальних матеріалів, які послаблюють випромінювання на 20-30 дБ

- Спеціальні окуляри зі скла з провідною плівкою двоокису олова для захисту очей

- Використання засобів індивідуального захисту лише у випадках, коли інші заходи неможливо застосувати

Лікувально-профілактичні заходи:

- Професійний відбір персоналу для роботи у зонах підвищеного ЕМП

- Дотримання регламентованих режимів праці та відпочинку

- Регулярні медичні огляди персоналу

- Проведення профілактичних заходів щодо зменшення впливу ЕМП

Мінімізація енергетичного навантаження на навколишнє середовище досягається через впровадження енергоефективних технологій та заходів:

Енергоефективні технології:

- Використання сучасних серверів та обладнання з високою енергоефективністю (класи A, A+, A++)

- Впровадження систем автоматичного відключення обладнання при неактивності (спящий режим)

- Оптимізація охолоджуючих систем ЦОД (центрів обробки даних) з використанням технологій вільного охолодження

- Застосування гідротехнічних рішень для охолодження серверного обладнання з використанням циркуляції охолоджувальної рідини

Відновлювальні енергетичні джерела:

- Встановлення сонячних панелей (фотоелектричних систем) на дахах ЦОД та офісних приміщень

- Використання вітряних турбін для генерування електроенергії

- Підключення до «зелених» тарифів енергопостачальників, які використовують відновлювальні джерела

- Активна участь в програмах компенсації вуглецевого сліду

Енергетичний аудит та контроль:

- Регулярне проведення енергетичних аудитів для ідентифікації джерел зайвого енергоспоживання

- Встановлення систем моніторингу енергоспоживання в реальному часі

- Розробка та реалізація планів енергозбереження

- Навчання персоналу правилам енергозбереження та ефективного використання обладнання

Правильне управління електронними відходами (e-waste) є критично важливою частиною охорони навколишнього середовища, оскільки комп'ютерне обладнання містить токсичні речовини.

Склад та токсичність електронних відходів:

- Важкі метали: свинець, ртуть, кадмій, хром, нікель — можуть накопичуватися в організмі та спричинити серйозні захворювання

- Галогені: використовуються в вогнегасниках, при розкладанні утворюють токсичні вещества

- Органічні забруднювачі: стійкі органічні забруднювачі (POPs), які не розкладаються в довкіллі

- Пластикові матеріали: можуть розкладатися сотні років, забруднюючи довкілля

Класифікація електронних відходів:

- Комп'ютери та периферійні пристрої (миші, клавіатури, сканери)
- Сервери та мережеве обладнання (маршрутизатори, комутатори)
- Елементи живлення та батарейки
- Кабелі та з'єднувальні матеріали
- Монітори та дисплейні засоби
- Принтери та копіювальні машини

Заходи щодо мінімізації електронних відходів:

- Подовження терміну експлуатації обладнання через своєчасне технічне обслуговування
- Розумна закупівельна політика з урахуванням циклу життя обладнання та його утилізованості
- Укладання контрактів із виробниками на зворотній прийом застарілого обладнання
- Використання лізингових схем замість прямої закупівлі обладнання
- Пожертвування застарілого, але функціонального обладнання освітнім установам або благодійним організаціям

Утилізація та переробка:

- Передача застарілого обладнання ліцензованим підприємствам з переробки електронних відходів
- Розбирання обладнання та сортування компонентів для подальшої переробки
- Безпечне видалення токсичних речовин (ртуть зі ламп, свинець зі припою, кадмій з батарей)
- Повернення цінних матеріалів (мідь, золото, срібло, алюміній) у виробничий цикл
- Утилізація пластику та інших матеріалів через спеціалізовані процеси переробки

Парадоксально, але цифровізація та розвиток інформаційних технологій можуть значною мірою сприяти охороні навколишнього середовища:

Екологічні переваги діджиталізації:

- Скорочення витрати паперу: через державну ЕкоСистему в Україні було збережено близько 880 дерев завдяки скоротженню обсягу паперових документів на 7,5 млн аркушів лише за один рік
- Зменшення обсягу транспортування: цифровий обмін документами скорочує потребу в фізичному транспортуванні, зменшуючи викиди парникових газів
- Оптимізація виробничих процесів: використання цифрових систем контролю дозволяє оптимізувати виробничі процеси та зменшити витрати ресурсів
- Скорочення часу прийняття управлінських рішень: цифрові системи дозволяють приймати рішення швидше та на основі більш точних даних

Системи моніторингу довкілля з використанням сучасних ІТ:

- Геоінформаційні системи (ГІС): для аналізу просторових даних про стан довкілля
- Дистанційне зондування земної поверхні: для оцінки змін рослинного покриву, водних ресурсів, забруднення
- Системи контролю забруднення: автоматизовані системи моніторингу атмосфери, водних ресурсів та грунту
- Аналіз та прогнозування екологічних ризиків: використання штучного інтелекту та машинного навчання
- Системи оповіщення про екологічні загрози: автоматичні системи ЕкоЗагроза, що повідомляють про забруднення та небезпеки

Управління природними ресурсами за допомогою цифрових технологій:

- Цифрові системи обліку та контролю добування мінеральних та енергетичних ресурсів
- Оптимізація розподілу водних ресурсів з врахуванням попиту та наявності
- Системи контролю лісокористування та лісовідновлення
- Моніторинг біорізноманіття та охоронюваних територій
- Системи управління твердими побутовими відходами з оптимізацією

логістики збирання та переробки

6.3 Нормативно-правова база охорони навколишнього середовища

- ISO 14001:2015 — Система управління навколишнім середовищем. Вимоги та керівництво щодо застосування
- ISO 14004 — Система управління навколишнім середовищем. Загальне керівництво щодо принципів, систем та способів впровадження
- ISO 14040, 14044 — Оцінка життєвого циклу продукту
- Конституція України (стаття 50) — право кожного громадянина на сприятливе довкілля
- Закон України «Про охорону навколишнього природного середовища» — основний закон у сфері охорони довкілля
- Закон України «Про відходи» — регулює питання управління побутовими та промисловими відходами
- Закон України «Про охорону атмосферного повітря» — вимоги щодо контролю забруднення атмосфери
- Закон України «Про охорону земель» — вимоги щодо охорони земельних ресурсів

6.4. Політика організацій щодо охорони навколишнього середовища

Основні принципи:

- Дотримання законодавства України та міжнародних стандартів при здійснені діяльності
- Постійна оцінка, покращення та підвищення результативності у сфері охорони навколишнього середовища
- Попередження та мінімізація негативного впливу на довкілля

- Забезпечення відкритої та прозорої комунікації з питань охорони навколишнього середовища з громадськістю та органами влади
- Співпраця з постачальниками, клієнтами та партнерами щодо охорони довкілля

Цілі політики охорони навколишнього середовища:

- Раціональне та збалансоване використання енергетичних та природних ресурсів
- Впровадження енергоефективних та ресурсоефективних технологій
- Навчання та розвиток персоналу у сфері охорони навколишнього середовища
- Відповідальна проектна діяльність з оцінкою впливу на довкілля
- Контроль за дотриманням третіми сторонами (підрядники, партнери) вимог законодавства

6.5. Моніторинг та контроль впливу на навколишнє середовище

Система моніторингу повинна включати:

Контроль викидів забруднюючих речовин в атмосферу від генераторів та систем вентиляції [27].

- Моніторинг використання та якості води, скидів стічних вод
- Аналіз утворення, накопичення, зберігання та руху електронних та інших відходів
- Вимірювання рівнів електромагнітного поля в приміщеннях та навколо них
- Оцінку енергоспоживання та вуглецевого сліду організації
- Оцінку впливу на біорізноманіття та екосистеми в районі розташування об'єктів

Документування результатів:

- Ведення реєстрів викидів та скидів забруднюючих речовин
- Звіти про управління та утилізацію відходів
- Записи результатів моніторингу ЕМП та енергоспоживання
- Аналіз тенденцій та розробка коригуючих дій
- Звітність перед громадськістю та органами влади про стан охорони довкілля

ВИСНОВКИ ДО РОЗДІЛУ 6

Охорона навколишнього середовища при управлінні кіберінцидентами у критичній інфраструктурі представляє собою комплексне завдання, що вимагає впровадження як традиційних природоохоронних заходів, так і сучасних цифрових рішень. Мінімізація впливу на довкілля через раціональне використання енергії, правильне управління електронними відходами, захист від електромагнітних полів та впровадження екологічно свідомих практик є важливою складовою корпоративної відповідальності.

Поєднання технічних (інженерно-технічних), організаційних та адміністративних заходів дозволяє досягти не тільки поліпшення екологічної ситуації в регіонах розташування об'єктів критичної інфраструктури, але й підвищення економічної ефективності діяльності організацій. Вищі керівники, керівники структурних підрозділів, всі працівники несуть спільну відповідальність за реалізацію принципів сталого розвитку та охорони навколишнього середовища.

ВИСНОВКИ

На основі проведених досліджень в кваліфікаційній роботі та отриманих практичних результатів можна зробити наступні висновки:

Сформульовано концептуальну модель управління інцидентами для критичної інфраструктури (КІ). Встановлено, що для забезпечення кіберстійкості КІ необхідне поєднання операційної гнучкості (підхід NIST) із системним управлінням (ISO/IEC 27001). Аналіз міжнародного досвіду (ENISA, CERT-EU) та резонансних атак (Colonial Pipeline, енергосектор України) довів, що ізольовані системи захисту є неефективними. Критично важливою є централізована координація, налагоджений обмін даними про загрози (Threat Intelligence) та формалізовані процедури ескалації між операторами КІ та національними центрами реагування (CERT-UA).

Систематизовано ландшафт загроз та методи їх аналізу в умовах гібридної війни. Дослідження атак 2022–2024 рр. виявило домінування деструктивного шкідливого ПЗ та складних ланцюгових атак на енергетичний та державний сектори. Обґрунтовано доцільність застосування комплексних фреймворків моделювання загроз (STRIDE, PASTA, MITRE ATT&CK) та методик оцінки ризиків (кількісних та якісних). Це дозволяє перейти від реактивного захисту до проактивного зриву ланцюгів атаки (Kill Chain) на ранніх етапах.

Визначено технологічні обмеження існуючих підходів та шляхи їх подолання. Аналіз показав, що класичні моделі реагування мають «вузькі місця» через фрагментованість даних та ручну обробку інцидентів, що неприпустимо в умовах швидкоплинних криз. Доведено необхідність інтеграції тріади SOC–SIEM–SOAR, де автоматизація рутинних дій та використання алгоритмів AI/ML є ключовими факторами для зменшення часу реагування та усунення людського фактору при обробці типових загроз.

Розроблено та обґрунтовано комплексну систему моніторингу та реагування. Запропоноване рішення, що об’єднує централізоване збирання журналів, кореляцію подій та превентивне сканування вразливостей, дозволило сформувати

цілісний контур безпеки. Практична реалізація системи продемонструвала можливість ефективного виявлення складних багатовекторних атак. Впровадження аналітичних панелей dashboards та стандартизація процесів тріажу забезпечили прозорість ситуаційної обізнаності та скорочення ключових метрик ефективності (MTTD та MTTR).

Забезпечено правові та організаційні умови для персоналу та довкілля. Встановлено, що надійність роботи центрів управління кіберінцидентами (ЦУКІ) залежить не лише від технологій, а й від умов праці персоналу. Розроблені заходи з охорони праці (нормалізація мікроклімату, освітлення, психологічне розвантаження) спрямовані на підтримку високої концентрації уваги операторів під час кризових ситуацій. Також визначено, що інфраструктура кіберзахисту має відповідати принципам сталого розвитку, зокрема через енергоефективність та належну утилізацію електронних відходів.

У підсумку, запропонований у роботі комплексний підхід, який поєднує вдосконалені організаційні моделі, автоматизовані технічні засоби виявлення та реагування, а також належне забезпечення умов праці, дозволяє суттєво підвищити рівень захищеності об’єктів критичної інфраструктури від сучасних кіберзагроз, мінімізуючи ризики для національної безпеки та економіки держави. Таким чином поставлені завдання виконано.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кузьменко В. В. Оцінювання ефективності управлінських рішень у кризових умовах для телекомунікаційної галузі України // Актуальні питання економічних наук. – 2025. – № 12. – [Електрон. ресурс]. – Режим доступу: https://a-economics.com.ua/index.php/home/article/view/577.

2. ISO/IEC 27000. Серія стандартів // ООО «ІНТЕРСЕРТ-УКРАЇНА» [Електрон. ресурс]. – Режим доступу: https://intercert.com.ua/articles/regulatory-documents/210-iso-27000.

3. Про критичну інфраструктуру : Закон України від 16 листопада 2021 року № 1882-IX [Електрон. ресурс] // Відомості Верховної Ради України. – 2021. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20 (станом на 05.12.2022).

4. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матер. міжнар. експерт. нарад / за заг. ред. О. М. Суходолі; упоряд.: Д. С. Бірюков, С. І. Кондратов. – К. : НІСД, 2015. – 176 с.

5. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII [Електрон. ресурс] // Відомості Верховної Ради України. – 2017. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19 (станом на 17.08.2022).

6. SCADA-система [Електрон. ресурс] // OPEKS energysystems. – Режим доступу: https://opeks.ua/ua/scada-sistema/ (дата звернення: 31.10.2025).

7. CRAMM [Електрон. ресурс] // ENISA. – Режим доступу: https://www.enisa.europa.eu/topics/riskmanagement/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html (дата звернення: 31.10.2025).

8. MITRE ATT&CK® [Електрон. ресурс]. – Режим доступу: https://attack.mitre.org/ (дата звернення: 31.10.2025).

9. Witcher R. Threat Modeling Methodologies: STRIDE, PASTA, and DREAD Explained [Електрон. ресурс] // Destination Certification. – 2025. – 25 Oct 2025. – Режим доступу: https://destcert.com/resources/threat-modeling-methodologies/ (дата звернення:

31.10.2025).

10. Bain T. Common Vulnerability Scoring System (CVSS) [Електрон. ресурс] // VulnCheck.–2024.–Режим доступу: https://www.vulncheck.com/blog/common-vulnerability-scoring-system (дата звернення: 31.10.2025).

11. Ukrainian CERT details malicious plan by Sandworm group to disrupt critical infrastructure facilities [Електрон. ресурс] // Industrial Cyber. – 23 Apr 2024. – Режим доступу: https://industrialcyber.co/critical-infrastructure/ukrainian-cert-details-malicious-plan-by-sandworm-group-to-disrupt-critical-infrastructure-facilities/ (дата звернення: 31.10.2025).

12. What Is the Cyber Kill Chain? [Електрон. ресурс] // Microsoft Security. – Режим доступу: https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain (дата звернення: 31.10.2025).

13. Коусса Ш. Comparison of STRIDE, DREAD & PASTA [Електрон. ресурс] // Software Secured Blog. – 15 черв. 2023. – Режим доступу: https://www.softwaresecured.com/post/comparison-of-stride-dread-pasta (дата звернення: 31.10.2025).

14. Гнатюк В. О., Зандер К. Ю. Методика формування структури центру збирання та оброблення даних під час моніторингу стану об’єктів критичної інфраструктури // Інфокомунікаційні та комп’ютерні технології. – 2025. – № 1. – С. 9–17.

15. Talabuev Y. Створіть свій план реагування на інциденти [Електрон. ресурс] // Colobridge Blog. – 26 трав. 2025. – Режим доступу: https://blog.colobridge.net/uk/2025/05/comprehensive-guide-steps-to-build-an-incident-response-plan-ua/ (дата звернення: 31.10.2025).

16. Матвійчук-Юдін О.О. Інноваційні методи захисту від соціально-інженерінгових атак : тези доп. Міжнар. наук.-практ. конф. здобувачів вищої освіти і молодих учених «Політ. Сучасні проблеми науки». – Київ, 2024. – Т. 2. – С. 44-49.

17. Vulnerability Scanning: Identifying Vulnerabilities with Regular Checks [Електрон. ресурс] // Hostragons Blog. – Режим доступу: https://www.hostragons.com/en/blog/vulnerability-scanning/ (дата звернення:

31.10.2025).

18. Смірнова Т. Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави // Кібербезпека: освіта, наука, техніка. – 2025. – Т. 2, № 30. – С. 195–208.

19. Федик В. Р., Денисенко Г. В. Теоретико-методологічні підходи до управління ризиками кібербезпеки на об’єктах критичної інфраструктури: реагування на кіберінциденти та менеджмент кризових ситуацій // Інформація і право. – 2024. – № 1 (48). – С. 195–202 (орієнтовно).

20. Мойко О., Кочин В., Борисова К., Тімошин А. Кібербезпека критичної інфраструктури та державна безпека // UNIVERSUM. – 2025. – № 3 (33). – С. 166–179.

21. Шульга В. П., Іванченко Є. В., Вишневська Н. С., Бербер А. С. Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави // Сучасний захист інформації. – 2024. – № 3.

22. Козанчин С. М., Яворська Т. В., Козик Н. В. Кібербезпека фінансових установ України [Текст] : магістерська робота. – Львів, 2022. – 74 с.

23. Гладчук М. В. Методи виявлення аномалій у великих даних для прогнозування кіберзагроз [Текст] : магістерська робота. – Тернопіль : ТНТУ ім. І. Пулюя, 2024. – 104 с.

24. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 72. – Ст. 2283.

25. ДСанПіН 3.3.2.007-98 Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин // Наказ МОЗ України від 10.12.1998 № 7. – Київ, 1998. – 24 с.

26. ДСанПіН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень // Наказ МОЗ України від 01.10.1997 № 382. – Київ, 1999. – 12 с.

27. ДСТУ EN 12464-1:2018 Світло та освітлення. Освітлення робочих місць. Частина 1. Робочі приміщення (EN 12464-1:2011, IDT) // Наказ Мінекономіки від 14.06.2018 № 138. – Київ: Держспоживстандарт України, 2018. – 68 с.