Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту

Кафедра кібербезпеки інформаційних систем, мереж і технологій

До захисту допущено
Кафедрою КІСМіТ протокол №____ від «___» грудня 2025 р.

завідувач кафедри _____ Марина ЄСІНА
(підпис) *(ім'я, прізвище)*
«___» грудня 2025 р.

Кваліфікаційна робота
здобувача другого (магістерського) рівня вищої освіти

Дослідження та порівняльний аналіз методів оцінки пріоритетності обробки кіберінцидентів з урахуванням визначених рівнів критичності
(назва роботи)

Спеціальність (спеціалізація) 125 «Кібербезпека та захист інформації»

Освітня програма «Безпека інформаційних і комунікаційних систем»

Виконавець _____ Аліса Біланович
(підпис) *(ім'я, прізвище)*

Науковий керівник _____ Марина Єсіна
(підпис) *(ім'я, прізвище)*

Харків – 2025

РЕФЕРАТ

Робота складається з 70 сторінок, 13 рисунків, 6 таблиць, 3 розділів та 28 джерел за переліком посилань.

Проведені у роботі дослідження спираються на публікації Національного інституту стандартів і технологій та інших міжнародних авторитетних видань, а також постанови і методичні рекомендації Кабінету Міністрів України та Адміністрації Державної служби спеціального зв’язку та захисту інформації України, які присвячені роботі з кіберінцидентами та створенню можливостей швидкого реагування на загрози комп’ютерній безпеці.

Наразі кіберінциденти залишаються недостатньо дослідженими для того, щоб спеціалісти усього світу мали єдине оптимальне визначення необхідних дій у випадку їх виникнення.

Актуальність роботи полягає у нестачі інформації про реагування на кіберінциденти та способи оцінки їх ступеня небезпеки.

Мета роботи – узагальнити та доповнити наявні відомості про оцінку кіберінцидентів та правильне реагування на виникаючі загрози, щоб забезпечити доступність і зрозумілість алгоритму захисту кіберпростору для всіх видів організацій у разі виявлення інцидентів.

Об’єктом дослідження є процеси та методики оцінки критичності кіберінцидентів, а також алгоритми реагування на загрози комп'ютерній безпеці.

Предметом дослідження є порівняльний аналіз методів визначення критичності кіберінцидентів, вдосконалення наявних в організації засобів виявлення та обробки інцидентів безпеки, практичні рекомендації щодо зменшення ймовірності появи несприятливих подій кібербезпеки.

У роботі докладно описані методи визначення критичності кіберінцидентів та засоби посилення захисту від загроз комп’ютерної безпеки.

У результаті роботи мета була досягнута: були проведені дослідження та порівняльний аналіз існуючих методів визначення критичності кіберінцидентів,

визначено актуальні рівні критичності кіберінцидентів для подій у кіберпросторі України, а також були сформовані практичні рекомендації посилення кібербезпеки для будь-яких видів організацій.

Подальші дослідження мають бути спрямовані на забезпечення доступності автоматизованих методів обробки кіберінцидентів з використанням машинного навчання та сценаріїв реагування і на дослідження можливостей із спробами розробки універсального ефективного методу пріорітезації кіберінцидентів, який буде релевантним для будь-якої організації.

Ключові слова: КІБЕРІНЦИДЕНТ, РІВЕНЬ КРИТИЧНОСТІ, ПРІОРІТЕЗАЦІЯ, РЕАГУВАННЯ, ОБРОБКА, КОМАНДА РЕАГУВАННЯ, ПЗ.

ABSTRACT

The work consists of 70 pages, 13 figures, 6 tables, 3 sections and 28 sources according to the list of references.

The research conducted in the work is based on publications of the National Institute of Standards and Technologies and other international authoritative publications, as well as resolutions and methodological recommendations of the Cabinet of Ministers of Ukraine and the Administration of the State Service for Special Communications and Information Protection of Ukraine, which are dedicated to working with cyber incidents and creating opportunities for rapid response to threats to computer security.

Currently, cybersecurity incidents remain insufficiently researched for specialists around the world to have a single optimal definition of the necessary actions in the event of their occurrence.

The relevance of the work lies in the lack of information on responding to cybersecurity incidents and methods for assessing their degree of danger.

The purpose of the work is to summarize and supplement the existing information on the assessment of cybersecurity incidents and the correct response to emerging threats in order to ensure the accessibility and clarity of the cyberspace protection algorithm for all types of organizations in the event of incidents.

The object of the study is the processes and methods of assessing the criticality of cybersecurity incidents, as well as algorithms for responding to computer security threats.

The subject of the study is a comparative analysis of methods for determining the criticality of cybersecurity incidents, improving the organization's means of detecting and processing security incidents, and practical recommendations for reducing the likelihood of adverse cybersecurity events.

The work describes in detail methods for determining the criticality of cybersecurity incidents and means of strengthening protection against computer security threats.

As a result of the work, the goal was achieved: research and comparative analysis of existing methods for determining the criticality of cybersecurity incidents were conducted, the current levels of criticality of cybersecurity incidents for events in the cyberspace of Ukraine were determined, and practical recommendations for strengthening cybersecurity for all types of organizations were formed.

Further research should be aimed at ensuring the availability of automated methods for handling cybersecurity incidents using machine learning and response scenarios and at exploring the possibilities of trying to develop a universally effective method for prioritizing cybersecurity incidents that would be relevant to any organization.

Keywords: CYBER INCIDENT, CRITICALITY LEVEL, PRIORITIZATION, RESPONSE, VULNERABILITY, RESPONSE TEAM, SOFTWARE.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

НКЦК РНБО	Національний координаційний центр кібербезпеки Ради національної безпеки і оборони України
ПЗ	програмне забезпечення
СБУ	Служба безпеки України
СОП	стандартні операційні процедури
ТТП	тактики, техніки та процедури
BYOD	Bring your own device – використання власного обладнання на підприємстві
CERT-CC	Computer Emergency Readiness Team Coordination Center – координаційний центр комп'ютерної групи реагування на надзвичайні ситуації
CERT-UA	Ukrainian Computer Emergency Readiness Team – комп'ютерна група реагування на надзвичайні ситуації України
CISA	Cybersecurity and Infrastructure Security Agency – агентство з кібербезпеки та безпеки інфраструктури
CVE	Common Vulnerabilities and Exposures – загальновідомі вразливості
CVSS	Common Vulnerability Scoring System – загальна система оцінювання вразливостей
DDoS	distributed denial-of-service attack – розподілена атака на відмову в обслуговуванні
EMM	enterprise mobility management – управління корпоративною мобільністю
IaaS	Infrastructure as a Service – інфраструктура як послуга
IDPS	Intrusion detection and prevention system – системи виявлення і попередження вторгнень

IP-адреса	Internet Protocol address – унікальний числовий ідентифікатор користувача
ML	machine learning – машинне навчання
NVD	National vulnerability database – Національна база даних вразливостей
OSI	open systems interconnection – взаємодія відкритих систем
PaaS	Platform as a Service – платформа як послуга
SaaS	Software as a Service – програмне забезпечення як послуга
SIEM	security information and event management – система управління інформаційною безпекою та подіями безпеки
SOAR	Security Orchestration, Automation and Response – оркестрація, автоматизація і реагування на загрози безпеки
SSH	Secure Shell – безпечна оболонка
TLP	Traffic Light Protocol – маркування конфіденційної інформації
UEBA	User and Entity Behavior Analytics – аналітика поведінки користувачів та активів
VPN	Virtual Private Network – віртуальна приватна мережа
ZTA	Zero-Trust Architecture – архітектура нульової довіри

ВСТУП

Дослідження кібербезпеки почалося майже одночасно зі створенням перших комп'ютерів та Інтернету у 1960-1970-х роках, проте перші серйозні зміни і впровадження розпочалися лише на початку 1990-х років. Саме на початку 90-х Інтернет став доступнішим та отримав широке поширення на території розвинених держав, через що з'явилися і неочікувані проблеми та ризики для користувачів. Наприклад, вони стикаються з появою кіберзагроз.

Найпершим кіберінцидентом вважають «Morris worm» [1]: аспірант Роберт Морріс в 1988 році створив і запустив у мережу ARPANET хробака. Хоча у студента не було намірів захопити дані мережі чи пошкодити їх – він випустив вірус від нудьги та з наукової зацікавленості, хробак встиг розповсюдитися на 6000 тогочасних комп’ютерів, спричинивши сповільнення роботи більшості наукових і військових центрів США. Збитки від непередбаченої кібератаки склали майже 100 мільйонів доларів. Саме після цієї події світові стало зрозуміло, що необхідно розвивати кібербезпеку.

Отже, одночасно із розвитком Інтернет-мережі постало і питання того, як забезпечити надійність і безпечність такого зв'язку. США ще на початку 20 століття побачила велику загрозу у відсутності законодавчої бази відносно кіберпростору. Президент та його адміністрація швидко визнали, що кіберзлочини і кібершпигунство становлять серйозну загрозу національній безпеці країни.

Для України розвиток кібербезпеки почався пізніше, адже широкого розповсюдження Інтернет набув лише у 2009 році, через 17 років після призначення країні власного офіційного домену. Проте, Інтернет для державних установ став доступним вже у 1995 році, що спонукало спеціалістів до аналізу мережі і створення можливостей захисту оцифрованої інформації. Відтак, історія Державного центру кіберзахисту почалася 01.01.2007 з моменту створення Державної служби спеціального зв’язку та захисту інформації України відповідно до Закону України «Про Державну службу спеціального зв’язку та захисту

інформації України». У 2009 році було створено окремий відділ Міністерства внутрішніх справ, який спеціалізувався на боротьбі з кіберзлочинністю, а вже у 2015 році була створена Кіберполіція (як структурний підрозділ Національної поліції). Окрім цих структур, на території України також почали функціонувати Ситуаційний центр забезпечення кібербезпеки при Службі Безпеки України (СБУ) та Національний координаційний центр кібербезпеки Ради національної безпеки і оборони України (НКЦК РНБО). Зі зростанням геополітичної напруги, особливо після повномасштабного вторгнення, кіберпростір став однією з бойових територій. Постійна загроза призвела до посилення заходів кіберзахисту і стала поштовхом для розширення кіберзахисних структур.

Незважаючи на такий стрімкий розвиток, на думку експертів рівень захищеності кіберпростору України залишається незадовільним. «Сприятливими чинниками» для цього є недостатня обізнаність та компетентність у питаннях кібербезпеки. Також відзначається, що велика частина населення не усвідомлює загроз, пов'язаних з кібербезпекою.

Ця робота спрямована на те, щоб забезпечити доступність і зрозумілість та обґрунтувати необхідність захисту кіберпростору для всіх видів організацій від кіберінцидентів.

Актуальність роботи полягає у нестачі інформації про реагування на кіберінциденти та способи оцінки їх ступеня небезпеки. Робота має узагальнити та доповнити наявні відомості про правила визначення рівнів критичності кіберінцидентів.

Завданням дослідження є порівняльний аналіз методів оцінки пріоритетності обробки кіберінцидентів з урахуванням визначених рівнів критичності та формування практичних рекомендацій щодо реагування на інциденти та зниження ризиків їхньої появи на підприємствах.

Відповідно до сформованого завдання було створено поетапний план досягнення цілей, який включає:

- аналіз підходів до визначення пріоритетності обробки кіберінцидентів/кібератак з урахуванням рівнів критичності;

- дослідження та аналіз нормативно-правової бази у сфері кіберінцидентів та рівнів критичності;
- дослідження та аналіз засобів та методів підвищення захищеності від кіберінцидентів;
- аналіз бази знань для виявлення кіберінцидентів MITRE ATT&CK;
- дослідження, аналіз та опис загальних правил обміну інформацією про кіберінциденти;
- дослідження, аналіз та опис методичних основ визначення пріоритетності заходів відновлення діяльності при реагуванні на кіберінцидент;
- формування висновків щодо здійсненої роботи.

1 ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ ТА ЇХ ОБРОБКА

1.1 Визначення кіберінциденту

Для правильного реагування на кіберінцидент необхідно чітко розуміти, які події на підприємстві або при особистому користуванні можна вважати інцидентами кібербезпеки.

Спостережувана подія у системі – така, як, наприклад, запит на доступ до файлу від користувача – це звичайна подія, яка не є інцидентом або несприятливим впливом.

Несприятлива подія відповідно є такою, що несе у собі негативні наслідки для функціонування системи: вимкнення світла, зникнення пакетів даних, збої у роботі тощо. Несприятлива подія, що викликана природніми явищами або відключеннями живлення, не вважається загрозою кібербезпеці. Несприятливі події, що спричинені навмисно (за людського впливу) є кібератаками [2].

Кіберінцидентом вважається будь-яка подія, яка порушує стале функціонування системи (або загрожує його порушенням) чи несе загрозу для безпеки інформації, розташованій у системі. Таким чином, усі види несприятливих подій вважаються кіберінцидентами. Не кожен кіберінцидент є кібератакою, проте кожна кібератака є кіберінцидентом.

Як приклад інцидентів комп’ютерної безпеки можна навести наступні події:

- працівник відкриває підозріле посилання на корпоративному девайсі, що дає змогу поширюватись шкідливому програмному забезпеченню, яке містилося за гіперпосиланням;
- зловмисник отримує доступ до конфіденційних даних та здійснює їхнє оприлюднення;
- зловмисник надсилає спам-запити у великому обсязі, через що виникають збої у системі тощо.

Наразі вже існує багато способів, за допомогою яких можуть бути визначені інциденти. Основним способом є впровадження системи виявлення і попередження

вторгнень (Intrusion detection and prevention system, IDPS) у поєднанні з антивірусним програмним забезпеченням. Також важливою складовою моніторингу є журнали активності.

Для вже відомих інцидентів комп'ютерної безпеки (зазвичай шкідливого програмного забезпечення, наприклад, вірусів) можуть бути описані сигнатури – рядки чи бітові шаблони даних, які дозволяють ідентифікувати загрозу в системі. Приклад сигнатури з тіла вірусу «Antivirus 2009 Plus.exe», зашифрованого під антивірусне програмне забезпечення [3]:

ABE423E3DD49F887E4883EF993F9C9628354C8A74E0C2613950CB27B9B705E64E5E139

Кіберінцидент може бути визначений і вручну, наприклад, якщо буде помічено файл із дивною назвою під час перевірки активних процесів робочого пристрою.

Варто вказати, що інциденти безпеки є дуже різноманітними: в той час як ознаки одного інциденту можна побачити без аналізу спеціаліста чи антивірусного ПЗ, інший інцидент може залишатися непомітним навіть після ураження більше, ніж половини даних у мережі.

Незважаючи на різноманітність реалізації кіберінцидентів, частіше за все вони мають схожі ознаки, за якими користувач може припустити наявність проблеми в системі:

- робота пристрою(-їв) сповільнюється;
- виникають збої під час виконання задач (вікна доводиться відкривати декілька разів, сторінки самостійно перенаправляються на інші матеріали, повідомлення та файли самостійно з'являються чи зникають в системі тощо);
- антивірус (якщо такий встановлено) самостійно відключається або не може здійснити перевірку файлів;
- журнал активності реєструє невдалі спроби авторизації незнайомого пристрою у мережі;

- проблеми з обліковим записом: користувач не може отримати доступ до системи за допомогою своїх даних; отримує повідомлення про підтвердження або спроби автентифікації, які ним не здійснювалися, або отримує повідомлення про успішний вхід до облікового запису з невідомого пристрою.

Більшість кіберінцидентів зазвичай мають лише декілька ознак з вищенаведеного переліку.

Зазначені вище ознаки інцидентів ще називають індикаторами, адже вони показують, що інцидент вже відбувся. Однак, існують і прекурсори інциденту – ознаки того, що інцидент може відбутися у майбутньому. Наприклад, прекурсором можна вважати погрози з невідомої електронної пошти чи облікового запису, у яких стверджується, що на організацію буде здійснено атаку за невиконання зазначених вимог (зазвичай вимоги стосуються певних сум грошей у якості «викупу» безпеки).

Найбільш поширеними джерелами виявлення інцидентів є сповіщення та журнали активності (табл. 1.1), але іноді прекурсори та індикатори можуть бути виявлені за допомогою відкритих джерел інформації:

- інформація з відкритих баз даних – деякі сайти та організації, наприклад, комп’ютерна група реагування на надзвичайні ситуації України (CERT-UA), координаційний центр CERT (CERT-CC), Національна база даних вразливостей (NVD) публікують нові виявлені вразливості та експлойти, оновлення вимог безпеки і засобів захисту;
- користувачі (як зовнішні, так і всередині організації) можуть помічати ознаки інцидентів і надсилати знайдену інформацію до відповідальних осіб.

Окрім цього, сторонні компанії можуть помітити незвичайні події безпеки і також повідомити про них організацію.

Таблиця 1.1 – Опис найбільш поширених джерел виявлення кіберінцидентів [4]

Найбільш поширені джерела виявлення кіберінцидентів	
Сповіщення системи безпеки	Журнали активності
• Система управління інформаційною безпекою та подіями безпеки (IDPS/SIEM): продукти SIEM та IDPS виявляють підозрілу активність на основі баз характерних ознак інцидентів та журналу системи, після чого автоматично формують відомості про неї: у звіт включається час і дата виявлення незвичайної події, джерела її надходження тощо. Таке джерело виявлення потребує постійного оновлення баз даних щодо сигнатур (шаблонів) інцидентів і кібератак у поєднанні з аналізом подій вручну, адже програмне забезпечення часто хибно позитивно розпізнає атаку, тоді як активність у мережі не була підозрілою.	• Централізоване журналювання: цілодобове ведення журналів активності для всіх операційних систем і служб організації для можливості аналізу трафіку та інформації стосовно облікових записів у будь-який момент часу. Порівняння активності служб, наприклад, протягом тижня, дозволить виявити інцидент у разі різких змін навантаження, робочого процесу тощо.

Продовження таблиці 1.1.

Найбільш поширені джерела виявлення кіберінцидентів	
Сповіщення системи безпеки	Журнали активності
• Антивірусне ПЗ: зазвичай таке програмне забезпечення базує свою оцінку небезпечності подій у системі на основі постійно оновлюваних баз даних щодо кіберінцидентів. Розробники регулярно перевіряють інформацію стосовно нових можливих сигнатур, так як від частоти і релевантності оновлюваних даних може залежати безпека девайсів і багатокористувацьких мереж.	• Журналювання потоків трафіку: відслідковування потоків інформації між хостами дозволяє швидко отримувати інформацію про зміни у процесі передачі даних: всього за декілька хвилин аналізу можна встановити, чи є аномальна активність інцидентом комп'ютерної безпеки.
• Програмне забезпечення перевірки геш-сум: під час модифікації файлів (видалення, додавання, спотворення інформації тощо) при збережені оновленого файлу його геш-сума скоріше за все також оновиться. Подібне ПЗ зберігає заздалегідь розраховані суми гешу для усіх файлів та регулярно порівнює збережені значення із сумами, розрахованими на момент поточної перевірки	

Щоб вчасно виявляти кіберінциденти (або запобігати їх появі) необхідно також розуміти можливі шляхи їх виникнення і регулярно власноруч проводити моніторинг системи (або налаштувати постійне відслідковування усіх процесів). Ще одним обов'язковим пунктом для швидкого коректного аналізу кіберінцидентів є присутність в організації або можливість залучення працівників із глибокими фаховими знаннями і значним досвідом у сфері кібербезпеки.

1.2 Реагування на кіберінцидент

Порядок опрацювання кіберінциденту виглядає наступним чином (рис. 1.1):

Рисунок 1.1 – Порядок опрацювання кіберінциденту

Виконання цієї послідовності дозволяє зменшити час відновлення системи, так як підозріла активність виявляться та обробляється швидше за рахунок постійного сканування системи.

Початковими діями будь-якої організації є оцінка ризиків, в результаті якої обираються та застосовуються засоби обмеження небезпеки. Ця практика дозволяє суттєво зменшити кількість можливих кіберінцидентів у майбутньому, проте, навіть маючи доступ до провідних методів захисту, для системи завжди зберігається залишковий ризик. Через це постійний пошук та виявлення порушень безпеки залишаються обов'язковими заходами.

Важливими компонентами опрацювання кіберінцидентів є відповідна команда реагування на події безпеки та політика, яка регулює процеси виявлення, обробки та усунення інцидентів з подальшим відновленням роботи мережі.

1.2.1 Команда реагування на кіберінциденти

Під час вибору майбутньої команди реагування на інциденти усі підприємства мають два основних варіанти [2]:

- команда, що складається з працівників компанії;
- аутсорсинг.

Розглядаючи варіант створення команди з працівників організації, варто зазначити, що структура команди також може бути різною.

Першим варіантом буде централізована команда реагування, яка обробляє інциденти усього підприємства в цілому. Така команда єдина для всієї структури організації, тому її оптимальність напряму залежить від розмірів компанії, кількості її філіалів, розподіленості ресурсів і т.д.

Другий можливий варіант – створення декількох команд для реагування на кіберінциденти, де кожна з команд відповідає за призначений їй сегмент (наприклад, одна команда відповідає за центр виробництва, інша – за центр реалізації продукції, чи у випадку поділу компанії на відділи – кожному відділу призначується власна команда реагування). Одразу декілька команд будуть ефективними для великих підприємств, так як дозволять більш ретельно відслідковувати події безпеки. Однак, навіть фактично не пов’язані між собою команди реагування (наприклад, одна знаходиться в Харкові, а інша – у Львові) мають бути частиною єдиної структури і мати можливість до постійного зв’язку між собою. Це необхідно для того, щоб здійснювати обмін досвідом про вже оброблені інциденти, а також мати можливість координації дій у випадку масштабної кібератаки, яка розповсюдиться за межі одного відділу організації.

Окрім аутсорсингу, досить розповсюдженим рішенням компаній є частковий аутсорсинг. Найбільш поширеним рішенням часткового аутсорсингу є передача моніторингу системи та ведення журналу активності сторонньому постачальнику

послуг безпеки. У такому випадку саме постачальник буде перевіряти роботу брандмауерів, сканувати мережу на наявність підозрілої активності та аналізувати вхідний і вихідний трафік. Якщо в результаті роботи якусь з подій буде визначено як інцидент безпеки, уся інформація стосовно неї буде передана безпосередньо команді реагування організації.

Іншим варіантом часткового аутсорсингу можна вважати залучення професіоналів за межами організації (наприклад, підрозділу CERT-UA) для допомоги з обробкою занадто масштабних кіберінцидентів, які компанія не здатна повністю усунути без сторонньої допомоги.

Повне передання реагування на аутсорсинг передбачає, що усі роботи з пошуку, виявлення, аналізу та усунення кіберінцидентів буде здійснювати стороння команда, як і керувати подальшими діями для відновлення роботи. Зазвичай до такого рішення звертаються організації, які не мають достатньої кількості кваліфікованих співробітників для формування власної команди реагування. Проте, організація залишається залученою у обробку кіберінцидентів, так як відслідковує і контролює дії аутсорсингової команди.

Важливо враховувати, що команда реагування на інциденти повинна бути цілодобово доступною. Якщо спеціалісти знаходяться не на об’єкті, в них все одно має бути можливість передивлятися процеси, що відбуваються у корпоративній мережі. Також має забезпечуватися постійний зв’язок між усіма членами команди та спосіб обміну повідомленнями з працівниками організації на випадок, якщо інцидент буде виявлено робітником, який не є складом команди реагування. Контакт у режимі реального часу часто потрібен і під час спільної роботи з іншими організаціями, наприклад, для відстеження атаки до її джерела [2].

Успіх команди реагування на інциденти залежить від участі та співпраці окремих осіб у всій організації.

1.2.2 Політика реагування на кіберінциденти

Після вибору оптимальної команди організація має створити відповідну політику стосовно реагування на інциденти. Остаточний зміст політики

індивідуальний для кожної організації, проте усі з політик повинні містити наступні розділи [5]:

- опис мети і завдання політики;
- сфера застосування політики;
- визначення інцидентів кібербезпеки та іншої термінології, пов’язаної з ними;
- визначення членів команди реагування на кіберінциденти та зазначення відповідних ролей;
- обов’язки, зобов’язання та повноваження команди реагування;
- вимоги та інструкції стосовно обміну інформацією про кіберінциденти і залучення сторонніх команд реагування в процесі обробки інциденту;
- зазначення попередньо розрахованої пріоритетності обробки можливих кіберінцидентів;
- стратегії реагування на інциденти різного рівня критичності;
- форма звітності;
- контакти керівництва та команди реагування на кіберінциденти.

Після формування команди і політики реагування необхідно впровадити спільний для усіх працівників план дій у разі кіберінциденту. Навчання усіх співробітників базовим правилам комп’ютерної безпеки і послідовності дій у разі підозрілої активності дозволить зменшити можливий руйнівний вплив кіберінцидентів. Наприклад, у випадку ураження одного корпоративного пристрою вірусом вчасне реагування і відключення його від спільної мережі допоможе запобігти розповсюдженню шкідливого програмного забезпечення та уникнути значних матеріальних збитків.

Політику реагування, план дій та якість знань працівників необхідно перевіряти принаймні щорічно, щоб переконатися, що подана інформація є актуальною, а основні ризики для організації визначені вірно.

Виходячи з вищезазначеного, усі процедури обробки інцидентів безпеки мають базуватися на політиці та плані реагування. Стандартні операційні процедури (СОП) є сукупністю заздалегідь визначених методів, технічних процесів

і способів контролю, які використовуються командою реагування на інциденти. СОП повинні бути достатньо вичерпними та детальними, щоб забезпечити відображення пріоритетів організації в операціях реагування. Крім того, дотримання стандартизованих відповідей має мінімізувати помилки, особливо ті, що можуть бути спричинені стресовими ситуаціями під час реагування на інциденти. СОП слід попередньо протестувати для підтвердження їхньої точності та корисності, а потім розповсюдити серед усіх членів команди.

1.2.3 Ресурси для аналізу та обробки кіберінцидентів

Однією зі складових роботи над кіберінцидентами, їх прекурсорами та індикаторами є обладнання і програмне забезпечення для їхньої обробки. Кожне підприємство має різні ресурси, проте для більшості організацій можна скласти наступний перелік:

- ноутбуки, комп’ютери, планшети та смартфони (як корпоративні, так і особисті);
- знімні носії (у числі яких має бути хоча б один порожній);
- пристрої резервного копіювання;
- цифрові робочі станції, що складаються хоча б з декількох жорстких дисків;
- системи відстеження та аналізу трафіку;
- програми для шифрування даних;
- програми гешування даних зі збереженням геш-сум;
- програмне забезпечення або методи для постійного моніторингу хостів і критично важливих активів;
- оперативний центр зв’язку (тимчасовий або постійник);
- резервні копії інформації та обладнання.

Перераховуючи основні необхідні ресурси організації, варто вказати і паперову документацію – на випадок блекаутів або занадто масштабних пошкоджень мережі чи цифрового обладнання підприємство повинне мати записні книжки, журнали активності, відомості, звітності та інші критично важливі

документи для забезпечення прискореного відновлення і постійного доступу до важливої інформації стосовно усунення подібних інцидентів.

1.3 Попередження інцидентів

Обробка кіберінцидентів є циклічною: під час аналізу та усунення інциденту часто необхідно повторювати обрані для виявлення дії, щоб перевірити інші брандмауери та хости на предмет того, чи не були вони також уражені внаслідок розповсюдження виниклої небезпечної події. Цикл обробки можна пришвидшити, якщо забезпечити достатню кількість засобів контролю, однак, кінцевою ціллю будь-якої організації завжди буде зниження загальної кількості кіберінцидентів. Хоча повне усунення інцидентів не є можливим, існують основні рішення, які значною мірою знижують ймовірність їхньої появи [6]:

- Навчання персоналу: працівники, що мають доступ до технічного обладнання і цифрових документів мають бути ознайомлені з головними прекурсорами та індикаторами інцидентів, щоб вони могли самостійно відмічати чи попереджати небезпечні ситуації комп’ютерної безпеки. Для персоналу, який безпосередньо працює у системі, використовує корпоративні девайси та застосунки, має проводитися додаткове навчання основним правилам безпеки в мережі, так як це дозволить уникнути деяких типів атак, наприклад, ураження вірусом через фішингове посилання з електронної пошти.
- Багаторівневий захист від ураження шкідливим програмним забезпеченням. Для цього пункту захист впроваджується на усіх рівнях мережевої моделі OSI (Open Systems Interconnection), як висвітлено в табл. 1.2.
- Оцінка ризиків. Під час оцінки ризиків необхідно розділити активи організації за їх важливістю і фінансовою цінністю, визначити ризики, що будуть найбільш вірогідними саме для цього підприємства, розподілити їх за рівнями критичності, впровадити постійний захист і моніторинг для

найбільш важливих ресурсів і ресурсів, необхідних для реагування у випадку інцидентів.

Таблиця 1.2 – Рівні моделі OSI з описом методів захисту безпеки для кожного рівня

7. Прикладний рівень 6. Рівень представлення 5. Сеансовий рівень Автентифікація користувачів, шифрування даних, захист від шкідливого ПЗ, додаткова перевірка вхідної інформації
4. Транспортний рівень Захист від атак на основі використання вразливостей протоколів TCP/IP шляхом фільтрації трафіку за номерами портів та шифрування інформації криптографічним протоколом TLS
3. Мережевий рівень Захист за допомогою фаєрволів і маршрутизаторів з імплементацією протоколів безпеки, забезпечення рівномірності трафіку для запобігання DDoS атакам
2. Канальний рівень Захист від спуфінгу та прослуховування, контроль доступу до мережі через VLAN і MAC-адреси
1. Фізичний рівень Захист від фізичного втручання, наприклад, ушкодження кабелів чи встановлення обладнання прослуховування

Ще одним рішенням, яке дозволить значно зменшити ризики виникнення кіберінцидентів є архітектура нульової довіри (zero trust architecture, ZTA). Концепція нульової довіри полягає у прийнятті факту того, що загрози для мережі існують як поза її межами, так і всередині неї. Модель нульової довіри постійно ставить під сумнів усі випадки неявної довіри, наприклад, передумови доступу

користувачів та завжди вимагає застосування політики надання найменшого необхідного доступу – тобто, кожен працівник отримує мінімальний доступ до інформації мережі, який є необхідним і достатнім для виконання його поточного завдання. Нульова довіра завжди спирається на припущення, що порушення безпеки інформації або її компрометація вже відбулися, через що довіра у системі ніколи не надається неявно і підлягає постійній оцінці і коригуванню. Фактично, архітектура нульової довіри не є готовим рішенням – для кожної організації вона має будуватися з урахуванням особливості її будови, розташування і кількості її ресурсів. Однак, для ZTA будь-якої компанії є загальні вимоги. Така архітектура має [7]:

- забезпечувати скоординований і постійний моніторинг системи;
- забезпечувати застосування принципу найменш привілейованого доступу до усіх даних, що зберігаються в мережі;
- завжди очікувати, що всі запити і потоки мережевого трафіку можуть бути уражені шкідливим ПЗ;
- завжди очікувати, що всі пристрої мережі можуть бути скомпрометовані;
- забезпечувати готовність до агресивних та скоординованих оборонних дій і контратак, швидкого реагування на відмови чи порушення функціонування критично важливих елементів архітектури;
- забезпечувати якнайшвидше відновлення контролю і робочих процесів після усунення інциденту.

Усі представлені методи зниження ризику дуже різняться за вартістю та ефективністю. На жаль, як вже було вказано раніше, навіть використання найкращих варіантів захисту не гарантує повну захищеність від появи інцидентів безпеки. Однак, якщо виникає одразу декілька кіберінцидентів, ресурсів організації може не вистачати на їх одночасну обробку. Через це необхідно мати можливість визначити рівень критичності (небезпечності) інциденту безпеки та приймати дії стосовно його усунення на основі результатів оцінки.

2 РІВНІ КРИТИЧНОСТІ КІБЕРІНЦИДЕНТІВ

Для реагування на кіберінцидент (або кібератаку) необхідно правильно визначати ступінь його небезпечності і кількість уражених даних. Від визначення деталей залежить обсяг ресурсів, що знадобляться на відновлення функціонування, а також вибір групи реагування і стратегії подолання проблеми. Зрозуміло, що в залежності від масштабності кіберінциденту, на нього буде витрачатися різна кількість часу. У випадку невірної оцінки події, шанси на мінімальні збитки від неї будуть знижуватися.

2.1 Методи визначення рівнів критичності кіберінцидентів

Від початку розвитку кібербезпеки до сьогоднішнього дня була розроблена не одна методика визначення рівнів небезпечності інцидентів. Деякі методики і метрики здобули визнання національного рівня, в той час як інші є більш локальними рішеннями. У цьому підрозділі будуть висвітлені методи оцінки різного рівня доступності, починаючи від найдешевших і найпростіших рішень, тоді ж як у наступному буде представлений варіант, що був визнаний міжнародним способом визначення рівнів критичності.

2.1.1 Класифікація на основі критичності активів

Метод оцінки кіберінцидентів на основі активів ґрунтується на попередній оцінці усіх активів організації. Оцінка зазвичай здійснюється за трьома критеріями критичності:

- форма функціонування (чи є активи матеріальними, нематеріальними або фінансовими);
- ступінь ліквідності (розрізняють ліквідні, середньоліквідні, малоліквідні та неліквідні активи);
- участь в обороті (активи можуть бути оборотними або необоротними).

Для державних об’єктів може також оцінюватись наявність чи відсутність секретності інформації активу.

У результаті такої оцінки інцидент, що виникне на критичному сервері бази даних отримає найбільший пріоритет, в той час як інцидент на робочому місці або новому обладнанні отримає значно меншу оцінку [8].

На перший погляд такий метод є доволі робочим і малокоштовним: для його впровадження немає необхідності у реконфігурації існуючої структури системи та її робочих процесів, а також не виникає необхідності у додатковому навчанні працівників. Однак, подібна оцінка критичності завжди буде залишатися суб’єктивною, адже вона не враховує тип виникаючого інциденту: перевантаження серверу запитами може виникнути без впливу зловмисної діяльності, наприклад, під час зростання попиту на лімітований товар, у той час як робочий девайс працівника може бути уражений атакою переміщення мережею. У такому випадку пріоритетність обробки кіберінцидентів буде визначено неправильно, через що атакуюче зловмисне ПЗ буде мати більше часу на розповсюдження.

2.1.2 Матриця ризику

Матриця ризику, на відміну від попереднього методу, зосереджується на оцінці самого майбутнього інциденту. Оцінка здійснюється за двома критеріями:

- ймовірністю виникнення інциденту;
- масштабами його впливу.

Масштаб впливу інциденту оцінюється за трьома головними принципами безпеки і захищеності інформації – конфіденційністю, цілісністю та доступністю.

Під час оцінки створюється матриця (рис. 2.1), у кожній комірці якої розміщується інцидент. Залежно від визначеної позиції інциденту робиться заключення стосовно пріоритетності його обробки. Зеленим відмічені найменш небезпечні інциденти, жовтим – інциденти середнього рівня значущості, червоним – критичні інциденти.

Такий метод визначення критичності є більш структурованим і використовує глибший аналіз загроз у порівнянні з класифікацією активів, однак, оцінка впливу

та ймовірності реалізації все ще залишається суб’єктивною. Однією з головних причин вибору цього методу для безпеки організацій є його низька вартість.

Імовірність виникнення	Дуже низький вплив	Низький вплив	Середній вплив	Високий вплив	Дуже високий вплив
Дуже низька					
Низька					
Середня					
Висока					
Дуже висока					

Рисунок 2.1 – Приклад матриці ризику

2.1.3 Скорингова система

Система очок, тобто скорингова система (scoring system) – це розширена версія матриці оцінки ризику, яка забезпечує більшу багатогранність оцінки кіберінциденту. Метод скорингу передбачає, що для кожного кіберінциденту буде визначено його скор (score) – кількісну оцінку, що складається із суми балів за визначеними критеріями [10]:

- критичність ураженого активу (зазвичай вимірюється від 1 до 10 балів);
- тип загрози (0-5 балів);
- поширеність інциденту (від 0 до 3 балів);
- чутливість уражених даних (від 1 до 10 балів).

Отриманий бал в результаті і визначає пріоритетність обробки кіберінциденту: якщо несприятлива подія в системі отримала менше 10 балів, то її обробка не вважається терміновою, у той час як подія зі скором більше 21 потребує негайного аналізу та усунення.

Для кожної організації можуть бути визначені власні додаткові критерії оцінки для забезпечення більш детального аналізу інцидентів безпеки. Наприклад, додатковим пунктом можуть бути прогнозовані фінансові витрати у разі успішності інциденту.

Частіше за все скорингова система створюється як звичайна послідовність пунктів – інциденти оцінюються вручну на основі документації стосовно критеріїв.

2.1.4 Алгоритми машинного навчання та автоматизації реагування на кіберінцидент

Машинне навчання (Machine learning, ML) є більш сучасним і динамічним підходом реагування на інциденти. Алгоритми машинного навчання дозволяють впровадити швидке виявлення аномалій у системі безпеки, що базується на аналізі усіх поточних та історичних даних стосовно кіберінцидентів і заздалегідь вивченої типової поведінки користувачів мережі.

ML-алгоритми навчаються на основі вже відомих кіберінцидентів, зокрема таких, які вже виникали в організації. Основна увага при навчанні надається оцінці потенційного впливу для кожного окремого кіберінциденту, їхнього можливого зв’язку між собою, швидкості та можливості їх розповсюдження. Таким чином, у випадку ураження мережі зловмисним шифрувальним ПЗ пріоритет такої події безпеки буде визначено як дуже критичний. Деякі організації можуть включати у навчальний процес і оцінку критичності ураженого активу. Навчання реагуванню на поведінку в мережі відбувається на основі аналітики поведінки користувачів та активів (UEBA) – створенні «базового профілю» користувача, програми та девайсу. Для кожного працівника системи і кожного активу відповідно складається профіль, у якому зазначаються усі можливі варіації «нормальної» поведінки [11]. Наприклад, якщо працівник із середнім рівнем доступу почне намагатися отримати доступ до ресурсів з грифом «таємно» або з робочого комп’ютера буде помічено завантаження нетипового обсягу даних, такі події автоматично будуть визначені підозрілими і додатково оброблені алгоритмами аналізу.

«Новим рівнем» машинного навчання є оркестрація, автоматизація і реагування на загрози безпеки (SOAR) – вона пропонує покращену автоматизацію та координацію процесів обробки інцидентів кібербезпеки. SOAR є набором програмних засобів та інструментів безпеки, що об’єднує дані про існуючі загрози і поточні процеси в єдиний автоматизований цикл перевірки мережі. При надходженні оповіщення платформа SOAR автоматично виконує серію запитів до різних систем: перевіряє репутацію IP-адреси – унікального числового ідентифікатора користувача в базах даних загроз, визначає власника порушеного активу, перевіряє наявність відповідних вразливостей (CVE), аналізує геш-суми файлів тощо [12]. Наприклад, повідомлення про підозрілі дії в системі з IP-адреси, яка вже була раніше визнана як ворожа, буде оцінено як інцидент дуже високого рівня критичності автоматично без людського впливу. Для низького та середнього рівня інцидентів безпеки SOAR дозволяє автоматизовувати дії реагування, повністю усуваючи проблему і забезпечуючи подальше відновлення робочих процесів без втручання працівників. Зазвичай, для цих рівнів застосовується блокування IP-адрес у міжмережевому екрані, ізоляція заражених хостів та анулювання скомпрометованих облікових записів. Це звільняє час команди реагування, дозволяючи їй зосередитись виключно на найбільш пріоритетних кіберінцидентах, що потребують глибокого аналізу та гнучкого мислення.

Ще однією значущою особливістю SOAR є можливість створювати сценарії реагування (у англомовній документації вони називаються «playbooks») – заздалегідь розроблені і описані послідовності дій при реагуванні на інцидент безпеки [12]. Наприклад, сценарій може бути записано наступним чином:

if (рівень критичності = високий && важливість активу = висока)

{ пріоритет = критичний;

запуск сценарію ізоляції активу;

відправка повідомлення про інцидент команді реагування; }

Найвищої дієвості автоматизованого реагування можна досягти шляхом об'єднання ML-алгоритмів усієї мережі з SOAR – усі процеси і потоки даних будуть проходити через єдиний цикл перевірки, який за необхідності буде ініціалізувати

збір додаткового контексту стосовно події, відміченої як підозрілої. Однак успішність такого підходу напряму залежить від якості і кількості навчального матеріалу для машинних моделей, який до того ж необхідно регулярно оновлювати і доповнювати.

Описані у цьому підрозділі методи пріоритезації кіберінцидентів є сильно розрізненими у складності і вартості впровадження. Вибір методики цілком залежить від можливостей конкретної організації.

2.2 Міжнародний стандарт CVSS

Загальна система оцінювання вразливостей (CVSS) – це відкритий стандарт, що містить у собі інформацію для передачі характеристик та розрахунку ступеня серйозності вразливостей програмного забезпечення. Метрики CVSS визнані на міжнародному рівні та рекомендуються до використання для організацій будь-яких розмірів і напрямків виробництва. CVSS складається з трьох груп метрик: базових, тимчасових та метрик середовища.

Базові метрики розглядають такі характеристики вразливостей, які є незмінними за часом і не залежать від середовища користувача, тимчасові описують характеристики вразливостей, що змінюються з часом, а метрики середовища відповідно висвітлюють характеристики, які є унікальними для кожного окремого середовища [13]. Кожна з груп метрик додатково розподіляється на підгрупи (рис. 2.2).

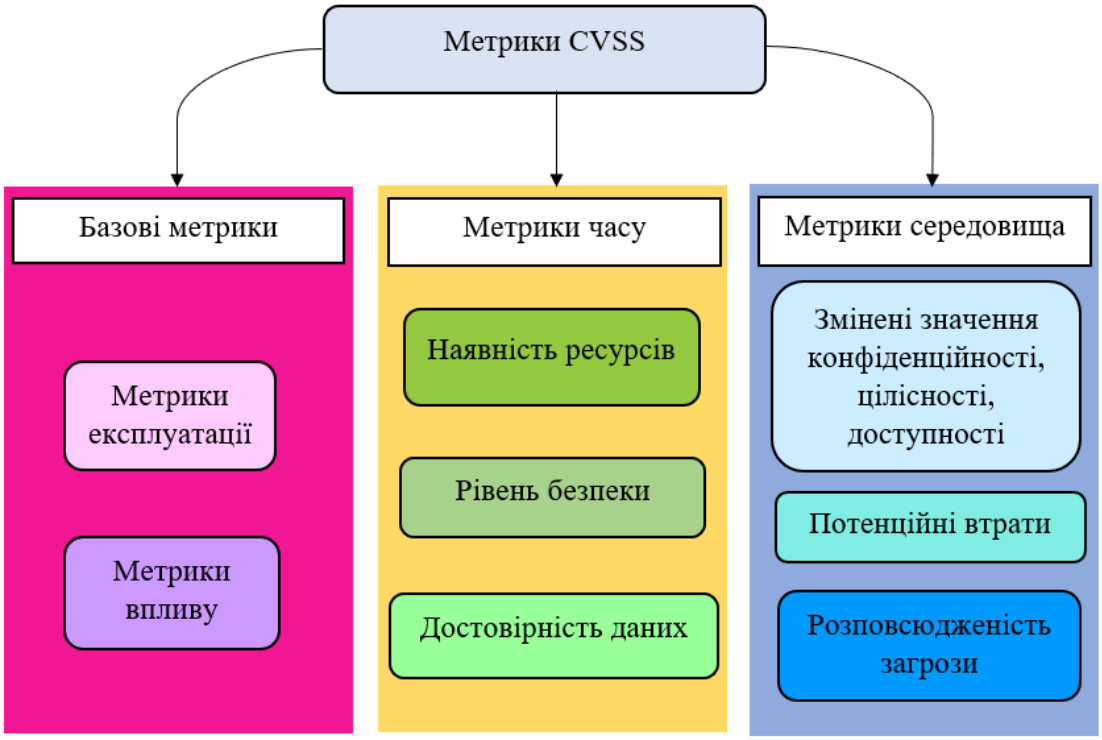

Рисунок 2.2 – Усі групи метрик CVSS

2.2.1 Базові метрики

Основною з усіх трьох груп метрик є базова – на її основі здійснюється первинна оцінка від 0 до 10 балів, яка пізніше може бути скоригована відповідно до особливостей конкретної організації (середовища) або часових характеристик. Зазвичай оцінка за базовими метриками здійснюється не самою організацією, а надавачем послуг кібербезпеки чи компанією, яка обслуговує вразливий продукт. Надану оцінку зазвичай мають скоригувати вже працівники організації, забезпечивши її відповідність поточним ризикам і ресурсам. Таким чином, вони можуть використовувати інформацію CVSS як вхідні дані для процесу управління вразливостями організації, який також враховує фактори, що не є частиною CVSS, щоб ранжувати загрози своїй технологічній інфраструктурі та приймати обґрунтовані рішення щодо усунення наслідків. Такі фактори можуть включати кількість клієнтів, грошові втрати через порушення робочого процесу, загрозу життю чи майну, або громадську думку щодо широко відомих вразливостей компанії. Усі подібні особливості організації виходять за рамки CVSS.

Базові метрики поділяються ще на дві додаткові групи, як було показано на рис. 2.2:

- метрики експлуатації;
- метрики впливу.

Метрики експлуатації відображають технічні засоби, за допомогою яких можна експлуатувати вразливість певного елемента мережі, а також визначають рівень складності, що необхідний для успішної реалізації загрози експлуатації. Під час оцінювання таких показників слід припускати, що зловмисник має поглиблені знання про слабкі місця цільової системи, включаючи загальну конфігурацію та стандартні механізми захисту (вбудовані брандмауери, контроль трафіку тощо). Засоби зниження впливу атаки, наприклад, такі, що контролюють умови надходження вхідних даних, повинні бути включені при оцінюванні показників середовища. Класифікація існуючих загроз навпаки не має впливати на базову оцінку – вразливий елемент варто оцінювати так, ніби він чутливий до усіх загроз організації.

При оцінці за метриками експлуатації розглядаються [13]:

- вектор атаки (рис. 2.3);
- складність атаки;
- необхідні привілеї;
- взаємодія з користувачем.

Як показано на рис. 2.3, існує чотири основні вектори атаки: з глобальної мережі, з локальної мережі, через віддалений вплив або доступ та через фізичний доступ до робочих пристроїв чи іншого обладнання. Атака через глобальну мережу зазвичай ніяк не пов’язана зі структурою мережі організації чи з працівниками компанії, вона експлуатує загальновідомі вразливості маршрутизаторів, програмного забезпечення, протоколів тощо. Наприклад, атакою з глобальної мережі можна вважати розподілену атаку на відмову в обслуговуванні (DDoS), адже для неї необхідний лише великий потік трафіку, якого можна досягти з будь-якої точки світу. При атаці у локальній мережі також може відбуватися перевантаження даними, однак джерело ураження має розміщуватися в самій

мережі організації: наприклад, атака має здійснюватися через корпоративну віртуальну приватну мережу (VPN).

Віддалений доступ – це атаки, доступ для яких було забезпечено через консоль чи мережевий протокол SSH.

Атаки через віддалений вплив в свою чергу фокусуються на взаємодії з вже авторизованим користувачем – наприклад, на пошту працівників надсилаються листи з фальшивими посиланнями, щоб реалізувати фішингову атаку.

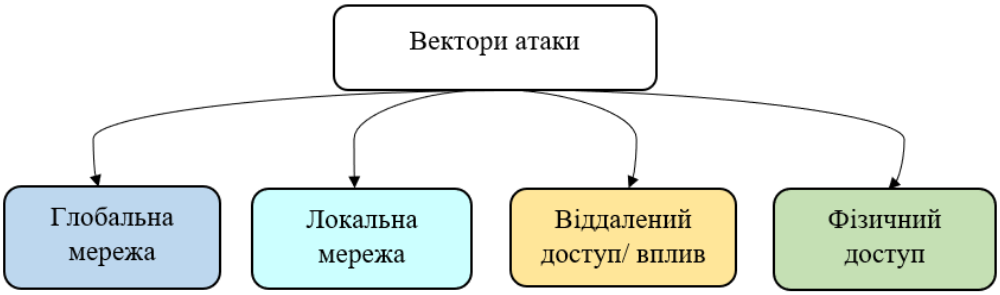

Рисунок 2.3 – Існуючі вектори атаки

Для складності атаки існує лише два можливих значення: низька чи висока складність. Низька складність передбачає, що зловмиснику не треба докладати зусиль для отримання доступу до вразливого елемента або те, що для існуючих вразливостей мережі не забезпечено достатнього рівня захисту. Відповідно, висока складність полягає в тому, що для успішності атаки треба докласти додаткових зусиль – наприклад, знайти спосіб для встановлення власного ПЗ перехоплення інформації.

Необхідні привілеї також стосуються зловмисників – під час аналізу визначається, який з трьох можливих рівнів необхідний для успішної реалізації атаки [14]:

a) низький – зловмиснику не потрібно проходити автентифікацію та/чи авторизацію в мережі;
b) середній – зловмиснику необхідно мати хоча б мінімальні привілеї користувача, такі як перегляд файлів і зміна власних налаштувань;

c) високий – зловмиснику необхідно мати високий рівень доступу, наприклад, адміністративний.

В свою чергу, метрика взаємодії з користувачем відображає вимогу участі людини-користувача, відмінного від зловмисника, в успішному зломі вразливого компонента. Ця метрика визначає, чи можна використати вразливість виключно за бажанням зловмисника, чи окремий користувач (або ініційований користувачем процес) повинен брати участь певним чином. Тобто, для цієї оцінки існує лише два можливих значення:

- участь користувача непотрібна;
- участь користувача є необхідною для успішної реалізації атаки.

Другий розділ базових метрик – метрики впливу – відображають прямі наслідки від успішного ураження вразливого елемента. Основними характеристиками, які оцінюються цією метрикою, є головна тріада принципів інформаційної безпеки – цілісність, доступність та конфіденційність. Для кожного з показників визначається три можливих рівня впливу: відсутній, низький та високий. Наслідки кожного рівня впливу описані у табл. 2.1.

Таблиця 2.1 – Наслідки впливу для цілісності, доступності та конфіденційності інформації [13]

Характеристика	Відсутній вплив	Низький вплив	Високий вплив
Цілісність	Цілісність інформації не було порушено.	Відбулася незначна модифікація даних, що не спричинила серйозного ураження.	Серйозні наслідки для ураженого елемента: втрата частини даних, зміна критичних даних або інша модифікація активів чи повне порушення цілісності для усіх даних на ураженій ділянці мережі.

Продовження таблиці 2.1.

Характеристика	Відсутній вплив	Низький вплив	Високий вплив
Доступність	Доступність інформації не було порушено.	Уражені дані залишаються постійно або частково доступними, зловмиснику не вдається повністю заборонити доступ до інформації.	Відбувається повна втрата доступності, в результаті чого зловмисник може повністю заборонити доступ до ресурсів ураженого компонента. Можливим варіантом є часткова втрата доступності, яка несе в собі важкі наслідки для мережі чи її елементів (наприклад, існуючі з'єднання у мережі зберігаються, але забороняється встановлення нових).
Конфіденційність	Конфіденційність інформації не було порушено.	Відбулася незначна втрата конфіденційності.	Повне порушення конфіденційності інформації чи її критичних значень (наприклад, виток паролів адміністратора безпеки).

2.2.2 Часові метрики

Метрики часу відповідають за такі параметри, що можуть змінюватися протягом робочого процесу. До таких характеристик належить наявність ресурсів для атаки, можливість підвищення безпеки вразливого елемента та достовірність отриманих даних.

Наявність необхідних ресурсів важко визначити з повною достовірністю, адже деякі зловмисники використовують власні напрацювання для здійснення атак. Проте, більшість баз даних стосовно експлойтів постійно оновлюються, що підвищує ймовірність якісної оцінки. Рівні «підготовленості» до атаки розподіляють на п’ять наступних критеріїв [13]:

- ресурси та можливості для атаки відсутні або існують лише теоретично;
- незначні можливості для атаки – код чи програмне забезпечення не завдають впливу для більшості (або всіх) активів організації або потребують значних модифікацій для успішного впливу на мережу;
- функціональний рівень – експлойт існує та його використання у більшості ситуацій гарантує успіх;
- високий рівень – експлойт існує та його використання забезпечує успіх за будь-яких обставин, розповсюдження доступне в автоматизованому режимі;
- наявність ресурсів та можливостей для атаки не доведено.

У випадку відсутності даних про ресурси і можливості зловмисників часова метрика не додається до загальної оцінки кіберінциденту, а кінцевий бал визначається на основі базової метрики.

Захищеність вразливого елемента також може змінюватись з часом – наприклад, після виявлення певних джерел атаки на елемент може бути впроваджено додаткові методи перевірки і аналізу. Ця характеристика під час оцінювання враховує і можливого надавача послуг безпеки (рис. 2.4).

Якщо змінити рівень захисту неможливо, оцінка за цим параметром не здійснюється.

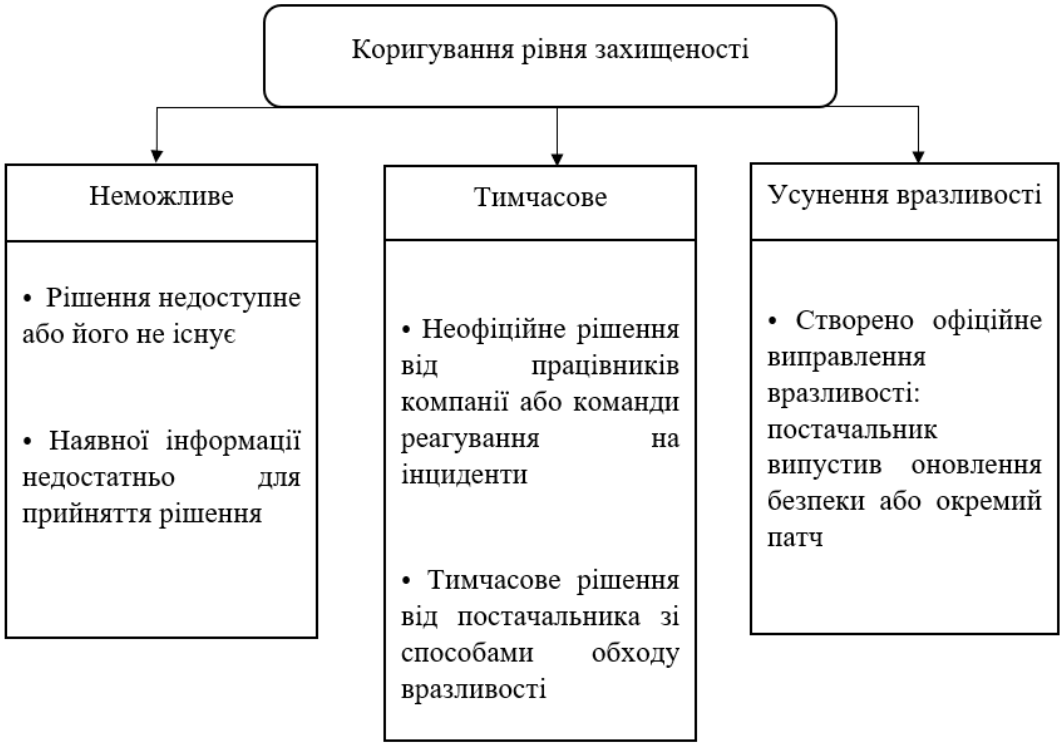

Рисунок 2.4 – Коригування рівня захищеності вразливого елемента

Третя характеристика часової метрики, тобто достовірність отриманих даних, завжди спирається на звіти стосовно ризиків та вразливостей, наявні у мережі. Іноді публікується лише існування вразливостей, але без конкретних деталей. Наприклад, вплив може бути визнаний небажаним, але його основна причина може бути невідомою. Пізніше вразливість може бути підтверджена дослідженнями, які показують, де може знаходитися вразливість, хоча дослідження може бути непевним. Зрештою, вразливість може бути підтверджена шляхом визнання автором або постачальником ураженої технології. Терміновість вразливості вища, коли існування вразливості відомо достовірно. Ця метрика також вказує на рівень технічних знань, доступних потенційним зловмисникам. У результаті достовірність інформації можна розділити на чотири можливі значення [13]:

- інформації про вразливість немає або недостатньо для формування звіту;

- існують повідомлення про вразливість, однак першопричина, результати впливу та інша необхідна інформація невідомі або звіти суперечать одне одному;
- точно відомо про наявність вразливості, однак не існує єдиної думки щодо причини її виникнення чи необхідних даних стосовно шкідливих ресурсів, які реалізують таку вразливість;
- існує повний опис вразливості або доступні вихідні коди, які забезпечують появу такої вразливості.

Можна побачити, що часові метрики впливають на оцінку ризику виходячи з даних стосовно робочих методів атак та існуючих експлойтів – зменшення ризику є можливим тільки у випадку офіційних оновлень безпеки від постачальників або відсутності можливих засобів створення кіберінцидентів на момент аналізу обраного елемента мережі.

2.2.3 Метрики середовища

Метрики середовища мають на увазі додаткові налаштування оцінки CVSS з огляду на власні оцінки організації: наприклад, включення рівня критичності активу до розрахунку кінцевих балів небезпечності інцидентів. У цій метриці розглядаються зміни щодо показників цілісності, доступності та конфіденційності інформації активу, потенційної шкоди і рівня розповсюдженості атаки [13].

Під розповсюдженістю атаки мається на увазі рівень ураження систем організації у разі її успішної реалізації: якщо під загрозою знаходиться більше 75% систем – рівень визначається високим, від 25% до 75% (включно) – середній рівень, від 1% до 25% (включно) – низький рівень. Відповідно, якщо загроз систем не існує або їх неможливо визначити, рівень розповсюдженості не застосовується при кінцевій оцінці.

При визначенні потенційної шкоди враховуються втрати або пошкодження обладнання, фінансові збитки та загрози життю працівників. Відповідно, у разі виникнення кіберінциденту можливі наступні рівні шкоди (рис. 2.5).

Рисунок 2.5 – Потенційні рівні шкоди у разі реалізації загрози

Повний вплив визначається відповідними метриками модифікованого базового впливу, які перерозподіляють вагу кожної характеристики з тріади безпеки [13]:

- інформації, щоб визначити вплив, недостатньо;
- втрата будь-якого з показників не призведе до значних наслідків для роботи організації та її працівників;
- втрата цілісності, доступності або конфіденційності інформації несе серйозні наслідки для робочих процесів та репутації компанії або її працівників;
- втрата будь-якого з показників веде до критично негативного впливу, який можна вважати катастрофічним.

Відповідно до рівнів наслідків порушення тріади безпеки модифікується попередньо сформована базова оцінка впливу на конфіденційність, доступність та цілісність. Відповідна оцінка залишається незмінною у разі неможливості визначення впливу з огляду на середовище.

2.2.4 Загальна шкала оцінки CVSS

Частіше за все використання рейтингів серйозності кіберінциденту CVSS (рис. 2.6) є необов’язковим, адже вони можуть відрізнятися від кінцевих балів, що включають усі особливості організації (такі як розташування, кількість ресурсів,

обсяги баз даних і т.д.). Загальна оцінка призначена для того, щоб полегшити правильне визначення небезпечності та пріоритетності роботи над вразливостями. Як вже було вказано раніше, кінцева оцінка кіберінциденту не може перевищувати 10 балів. Бали для рівнів критичності розраховуються у вигляді десяткових дробів, адже під час оцінки більшість метрик містять нецілочисельні значення від 0 до 1 (наприклад, офіційне усунення вразливості внаслідок випуску патча постачальником може бути оцінене як 0.87 балів з 1).

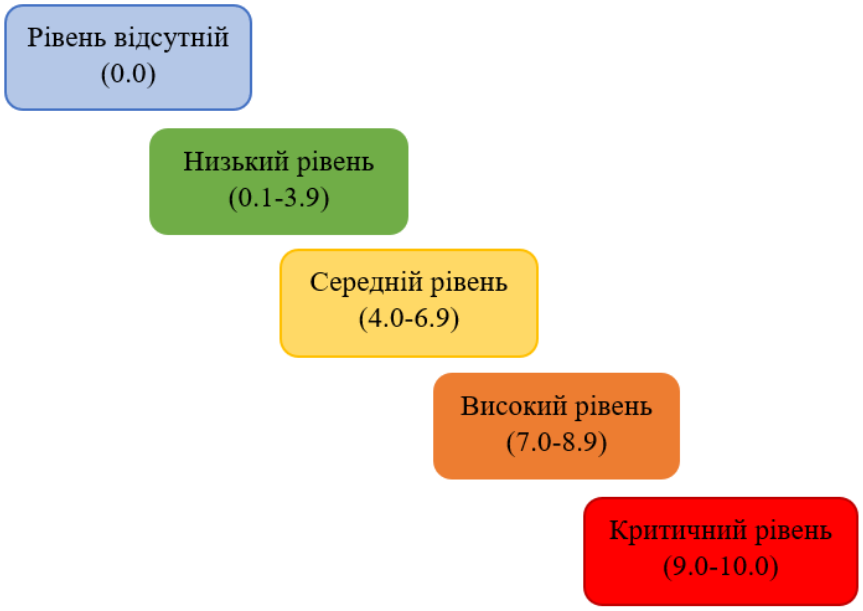

Рисунок 2.6 – Шкала оцінки критичності інциденту за CVSS

2.3 Покрокова пріорітезація за CISA

Агентство з кібербезпеки та безпеки інфраструктури (CISA) визначає наступну послідовність реагування на кіберінциденти [15]:

a) ідентифікація;

b) оцінення;

c) усунення;

d) звітність.

Процес реагування відбувається за сценарієм, що представлений на рис. 2.7. У цьому сценарії зелений колір відповідає за етап ідентифікації, синій – за етап оцінення, червоний – за етап усунення і чорний – за формування звітності.

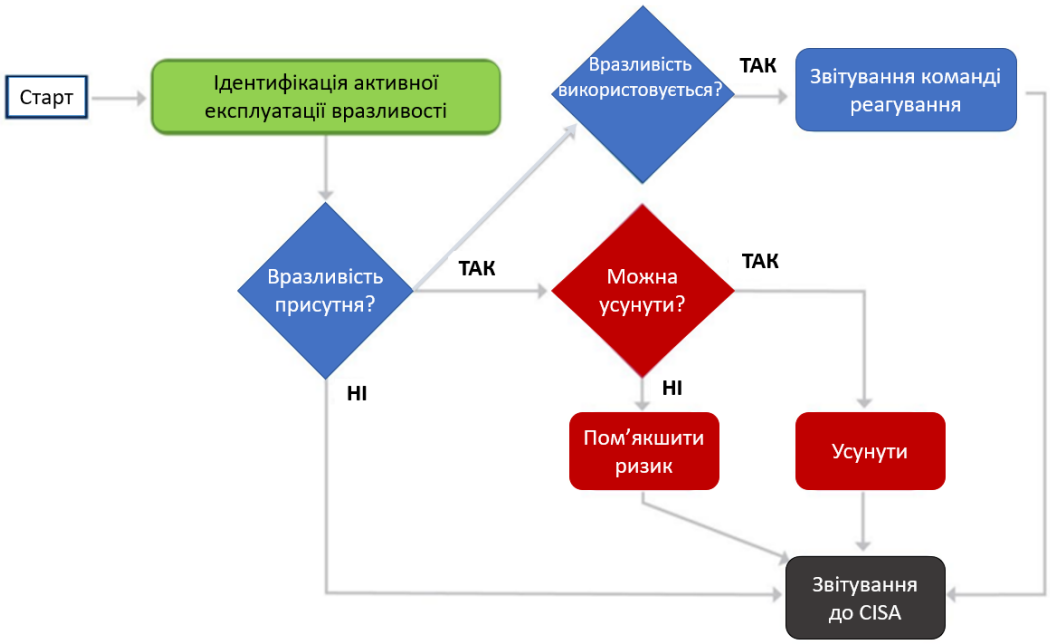

Рисунок 2.7 – Процес реагування на кіберінцидент за CISA

Для ідентифікації можливі три шляхи інформування про наявні вразливості чи загрози безпеці:

- ресурси CISA, наприклад, щотижневі оголошення зі зведеними даними про вразливості чи операційна директива BOD 22-01 CISA «Управління неприйнятним ризиком відомих вразливостей», яка постійно оновлюється з урахуванням вразливостей, що експлуатуються в реальних умовах;
- зовнішні ресурси, наприклад, Національна база даних вразливостей (NVD) або база даних і система класифікацій MITRE ATT&K;
- повідомлення з операційного центру безпеки організації.

Після визначення наявності або експлуатації вразливості у мережі, необхідно визначити критичність інциденту безпеки та важливість «уражених» ресурсів. Для цього CISA пропонує використовувати або власні метрики, або звернутися до методів, описаних у стандарті CVSS. Для активно використовуваних вразливостей рекомендується використовувати «швидкі процеси відповіді» (тобто автоматизовані сценарії реагування). У рідкісних випадках, таких як одноразові неправильні конфігурації, може знадобитися додаткове ручне сканування.

Директиви, які надає CISA, також можуть містити перелік конкретних технічних кроків для оцінки наявності вразливості.

Можливими варіантами з'ясування, чи була вразливість мережі використана, є наступні:

- пошук відомих індикаторів компрометації у системі;
- аналіз та завершення поточних процесів мережі;
- перевірка та аналіз усієї аномальної активності, наприклад, невдалих спроб доступу до інформації;
- співпраця зі сторонніми службами виявлення та реагування на інциденти або постачальниками послуг безпеки.

Наприкінці аналізу виявлення впливу за правилами CISA системі може бути призначено один з трьох станів [15]:

- система не вразлива;
- система вразлива, однак ознак експлуатації не було виявлено;
- система була скомпрометована – необхідно негайно розпочати усунення вразливості та відновлення після кіберінциденту.

На етапі усунення вразливості найчастішим вирішенням проблеми є встановлення виправлень для системи (патчів), однак можливі й інші варіанти, наприклад, ізоляція вразливих активів, обмеження доступу до них чи внесення регулярних змін до існуючої конфігурації мережі.

У випадках, коли патчів не існує, вони не були протестовані або не можуть бути негайно встановлені, можливими засобами зниження впливу на вразливість є лише засоби пом'якшення [15]:

- відключення послуг;
- переналаштування брандмауерів для блокування доступу;
- посилення моніторингу для виявлення експлуатації.

Щойно виправлення стануть доступними та їх можна буде безпечно встановити, засоби пом'якшення ризиків можна буде видалити, а виправлення – застосувати. У результаті роботи над усуненнями вразливостей для системи може бути призначений один з наступних станів [15]:

- система виправлена – вразливість усунено;
- ризики для вразливості системи пом’якшено;
- система залишається вразливою або скомпрометованою – заходів усунення або пом’якшення не було вжито.

Після усунення кіберінциденту та його наслідків необхідно додати додаткові засоби виявлення на рівні всього підприємства, щоб пришвидшити виявлення подібних атак противника, які були успішно виконані під час інциденту. Треба визначити та усунути «сліпі зони», щоб забезпечити належне покриття в майбутньому. Розширені методи захисту повинні розглянути можливість емуляції стратегічних планів захисту противника, щоб переконатися, що нещодавно впроваджені контрзаходи ефективні у виявленні або пом'якшенні спостережуваної активності. Це тестування має бути узгоджено з командою реагування на кіберінцидети та іншими працівниками відділу кібербезпеки, щоб переконатися, що їх не сплутають зі справжньою діяльністю зловмисника.

Кінцевим результатом реагування та пріоритезації кіберінцидентів за CISA має бути складання відповідного звіту про виявлену вразливість, спосіб її використання і впроваджені дії щодо її усунення або пом’якшення впливу на неї. Копії подібних звітів завжди мають надходити до CISA, адже вона повинна підтримувати обізнаність про стан реагування на вразливості, що активно експлуатуються. Ця обізнаність дозволяє допомогти іншим агентствам зрозуміти вплив вразливостей та скоротити час між отриманням інформації про вразливість чи кіберінцидент та діями щодо їхньої обробки. Варто враховувати, що можливості кіберзахисту дуже різняться в залежності від напрямку, розміру, фінансового становища та інших особливостей організацій. З цієї причини координація передбачає різний ступінь взаємодії між організацією та CISA. Для організацій із розвиненими можливостями захисту та реагування при інцидентах безпеки звітність та обмін інформацією є ключовими для допомоги іншим.

2.4 Порівняльний аналіз методів визначення критичності кіберінцидентів

Більшість розглянутих методів пріорітезації можуть бути впроваджені в організації одночасно, однак використання одразу усіх методів визначення критичності є технічно неможливим та неефективним. Для цього необхідно визначати, який з методів буде більш корисним для конкретної організації. Обрати один унікальний підхід до визначення критичності кіберінцидентів вкрай важко, однак для кожного з них існують свої переваги (табл. 2.2).

Таблиця 2.2 – порівняльний аналіз методів визначення критичності кіберінцидентів

Метод	Складність	Об’єктивність	Автоматизація	Переваги
Класифікація за активами	Низька	Низька	Низька	Простота
Матриця ризику	Низька	Середня	Низька	Наочність
Скорингова система	Середня	Вище середнього	Середня	Введення кількісної оцінки
CVSS	Висока	Висока	Висока	Відповідність стандартам, деталізація оцінки
SOAR/ML	Дуже висока	Висока	Дуже висока	Швидкість, адаптивність та масштабованість
CISA	Середня	Висока	Середня	Структурованість та можливість інтеграції з CVSS

Однак, не лише переваги методів мають впливати на кінцевий вибір організацій чи окремих користувачів. Варто враховувати і недоліки розглянутих методів визначення критичності.

Головним недоліком класифікації за активами та матрицею ризику є суб’єктивність – частіше за все, оцінка за цими методами здійснюється на основі власних висновків відповідального за пріорітезацію працівника.

Скорингова система та пріорітезація за CVSS вводять можливість кількісної оцінки на основі визначених в організації критеріїв. Проте, така оцінка вимагає великої кількості ручних обчислень і пропонує обмежені можливості для автоматизації процесів. До того ж, ці методи оцінки часто орієнтуються на визначені вразливостей мережі.

Найбільш ефективними для використання є методи SOAR з використанням ML та CISA: вони пропонують швидку об’єктивну оцінку кіберінциденту та дозволяють використання метрик CVSS у своїх процесах виявлення та обробки. Однак, такі методи є найбільш складними за рахунок поєднання великої кількості засобів і ресурсів. SOAR із забезпеченням якісних матеріалів для машинного навчання також є дороговартісною, що робить її недоступною для малих чи середніх підприємств.

2.5 Рівні критичності кіберінцидентів України

Для реагування на кіберінцидент (або кібератаку) необхідно правильно визначати ступінь його небезпечності і кількість уражених даних. Як вже було вказано раніше, від визначення деталей залежить обсяг ресурсів, що знадобляться на відновлення функціонування, а також вибір групи реагування і стратегії подолання проблеми. Зрозуміло, що в залежності від масштабності кіберінциденту, на нього буде витрачатися різна кількість часу. У випадку невірної оцінки події шанси на мінімальні збитки від неї будуть знижуватися.

Щоб досягти найбільшої ефективності, реагування на кіберінцидент має здійснюватися з постійним моніторингом його стану і з використанням заздалегідь визначених заходів відповідно до рівня небезпеки. Таким чином, одним з найголовніших етапів роботи над кіберінцидентом є правильне визначення його рівня критичності.

Станом на 2025 рік існує великий вибір методів визначення критичності кіберінцидентів, кожен з яких пропонує власні оцінки для виникаючої події кібербезпеки. Відповідна оцінка частіше за все є актуальною лише в контексті обраної метрики, адже різниця балів може бути значною: наприклад, сумарний бал скорингової системи для одного інциденту може становити 25 балів, у той час як оцінка за метриками CVSS складе 8.7 балів.

Якщо кіберінциденти можуть мати відношення до систем електронних комунікацій, систем управління технологічними процесами і безпеки інформаційних ресурсів країни, необхідно ввести чіткий розподіл критичності, який би міг використовуватися на державному рівні у випадку залучення одразу декількох команд реагування на події кібербезпеки або необхідності введення допоміжних заходів з боку інших країн. Щоб забезпечити подібну універсальність оцінювання та пришвидшити комунікації у разі виникнення кіберінцидентів, Кабінет Міністрів України затвердив постанову про «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі». У цій постанові були висвітлені порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі та рівні критичності кіберінцидентів, затверджені Адміністрацією Держспецзв'язку.

За постановою Кабінету Міністрів України виділяють 6 рівнів критичності кіберінцидентів [16]:

0) Білий (некритичний) – кіберінцидент/кібератака не загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів.
1) Зелений (низький) – кіберінцидент/кібератака загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, захищеності електронних інформаційних ресурсів та інших об'єктів кіберзахисту, проте не загрожує порушенню конфіденційності, цілісності та доступності інформаційних ресурсів держави або персональних даних громадян.

2) Жовтий (середній) – кіберінцидент/кібератака загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, захищеності електронних інформаційних ресурсів та інших об’єктів кіберзахисту, також створюються передумови для порушення конфіденційності, цілісності та доступності інформаційних ресурсів держави або персональних даних громадян, може здійснюватися вплив на надання основних послуг населенню.
3) Помаранчевий (високий) – кіберінцидент/кібератака загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, захищеності електронних інформаційних ресурсів та інших об’єктів кіберзахисту, внаслідок чого прогнозується помітній вплив на національну безпеку, обороноздатність, економічну безпеку, зовнішні відносини, основоположні свободи чи суспільну довіру або створюється потенційна загроза обмеження у наданні основних послуг населенню. На цьому рівні критичності може знадобитися залучення одразу декількох суб’єктів національної системи кібербезпеки для мінімізації збитків.
4) Червоний (критичний) – кіберінцидент/кібератака загрожує сталому функціонуванню декількох систем електронних комунікацій, систем управління технологічними процесами, захищеності електронних інформаційних ресурсів, інших об’єктів кіберзахисту, внаслідок чого прогнозується значній вплив на національну безпеку, обороноздатність, економічну безпеку, зовнішні відносини, здоров’я чи безпеку громадян або створюється реальна загроза обмеження у наданні основних послуг населенню. Реагування на цьому рівні потребує залучення ресурсів усіх основних суб’єктів національної системи кібербезпеки.
5) Чорний (надзвичайний) – кіберінцидент/кібератака загрожує сталому функціонуванню значної кількості систем електронних комунікацій, систем управління технологічними процесами, захищеності електронних інформаційних ресурсів, інших об’єктів кіберзахисту, внаслідок чого

відбувається невідворотній вплив на повноцінне функціонування держави або створюється загроза життю громадян України. Реагування на цьому рівні потребує максимальної державної участі, повного залучення всіх ресурсів основних та інших суб'єктів національної системи кібербезпеки.

Якщо стається декілька кіберіцидентів одночасно, черговість обробки кожного має розподілятися за додатковими пріоритетами:

- часом, необхідним на усунення кіберінциденту;
- прогнозованою кількістю ресурсів, необхідних для відновлення;
- джерелом виникнення кіберінциденту;
- критичністю впливу кіберінциденту на робочі та бізнес-процеси;
- наслідками впливу на інфраструктуру мережі;
- можливими наслідками для безпеки інформації (зокрема для її конфіденційності, цілісності та доступності);
- можливими наслідками для користувачів ураженої мережі.

У випадку виникнення інцидентів будь-якого рівня, окрім білого, організація має додатково повідомити про подію кібербезпеки до одного з трьох відповідних органів: НКЦК РНБО, СБУ або Національної поліції.

Окрім цього, для обробки кіберінциденту може бути залучена команда реагування CERT-UA, якщо дій власної команди реагування на кіберінциденти організації недостатньо або, якщо підприємство не є достатньо досвідченим у правильній обробці подій безпеки та подальшому відновленню робочих процесів.

Відповідна послідовність реагування і визначення необхідного державного органу представлена на рис. 2.8.

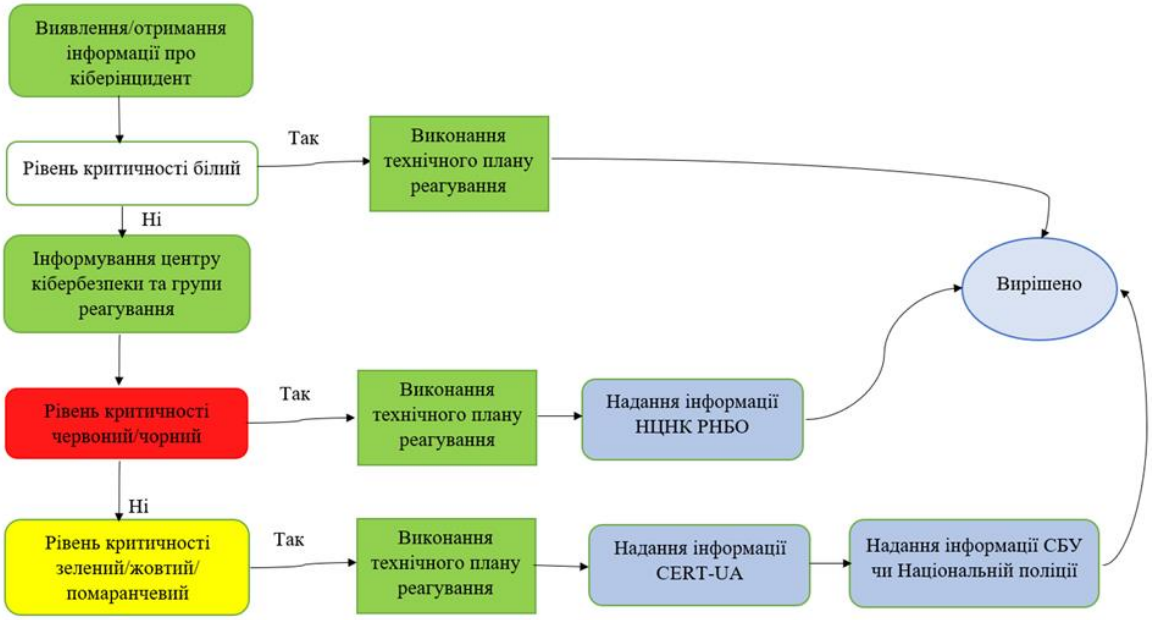

Рисунок 2.8 – Модель реагування на кіберінцидент в залежності від його рівня критичності

З моделі бачимо: у разі червоного або чорного рівня інциденту необхідно здійснити інформування Національного координаційного центру кібербезпеки. Важливо: інформація надається не лише про виникнення інциденту, але й про його можливі причини, наслідки, заплановані заходи нейтралізації.

У разі, якщо рівень критичності кіберінциденту визначено як зелений, жовтий або помаранчевий, необхідно інформувати CERT-UA. Служба безпеки інформується у разі того, якщо атака відбувається стосовно державних інформаційних ресурсів або критичних об’єктів інфраструктури, Національна поліція – у випадку вчинення правопорушення стосовно об’єкта приватного сектору.

Варто зазначити, що під час роботи над подією кібербезпеки заборонено повідомляти про використані засоби і вжиті методи до закінчення відновлювальних робіт будь-кому, окрім зазначених вище органів.

3 ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ЗМЕНШЕННЯ КІЛЬКОСТІ КІБЕРІНЦИДЕНТІВ, ВІДНОВЛЕННЯ СИСТЕМИ ТА ОБМІНУ ІНФОРМАЦІЄЮ

3.1 Посилення захисту від основних кіберзагроз організації

Забезпечення якісного захисту підприємства від будь-яких загроз інформаційній безпеці є критично необхідним, оскільки це безпосередньо впливає на його стійкість, фінансові операції та довіру клієнтів. Посилення захисту дозволить зменшити критичність виникаючих кіберінцидентів та кібератак, відповідно зменшуючи витрати ресурсів на їхнє виявлення, обробку, усунення та відновлення, а також значною мірою знизити «руйнівний» вплив від подібних несприятливих подій. Щоб максимально захистити організацію, необхідно звертати увагу на усі особливості її структури: кількість хостів та способи їх захисту, наявність корпоративних мобільних пристроїв, використання списків програм чи застосунків та використання хмарних сервісів обміну та зберігання даних.

3.1.1 Безпека мобільних пристроїв

Деякі організації можуть впроваджувати використання мобільних пристроїв для своїх робочих процесів. Частіше за все вони необхідні для доступу до конфіденційних даних чи корпоративної мережі, у деяких випадках використовуються для тестувань чи зберігання інформації. Оскільки подібні мобільні пристрої виконують повсякденні корпоративні завдання, вони регулярно обробляють, змінюють та зберігають конфіденційні дані. Хоча використання мобільних пристроїв та мобільних застосунків для доступу з будь-якого місця може суттєво підвищити продуктивність праці співробітників і пришвидшити процес прийняття рішень, а також ситуаційну обізнаність, ці пристрої несуть унікальні загрози для підприємства.

Щоб розуміти необхідні кроки при впровадженні захисту мобільних пристроїв, важливо знати їхній життєвий цикл в організації (рис. 3.1).

Рисунок 3.1 – Життєвий цикл корпоративних мобільних пристроїв

Загрози, пов’язані з впровадженням мобільних пристроїв [17]:

- експлуатація основних вразливостей у пристроях;
- втрата та крадіжка пристрою;
- використання вразливостей ланцюга поставок (наприклад, впровадження програм відстеження місцезнаходження між етапами передачі пристрою до кінцевого користувача);
- доступ до корпоративних ресурсів через неправильно налаштований пристрій;
- крадіжка облікових даних через фішинг;
- встановлення неавторизованих сертифікатів;
- використання ненадійних мобільних пристроїв;
- бездротове прослуховування;
- мобільне шкідливе програмне забезпечення;
- втрата інформації через незахищену конфігурацію блокування екрана;
- втрата даних через синхронізацію з іншими пристроями або сервісами;

- використання тіньових систем (тобто таких систем, які не були схвалені, керовані або навіть невідомі персоналу з кібербезпеки та відділу інформаційних технологій).

Організаціям рекомендовано впровадити наступні заходи для посилення безпеки мобільних пристроїв:

- аналіз загроз для мобільних пристроїв та будь-яких інформаційних систем, до яких здійснюється доступ з мобільних пристроїв;
- впровадження політики користування мобільними пристроями і перевірки мобільних застосунків;
- тестове впровадження мобільного рішення перед його запуском для масового використання;
- встановити усі визначені необхідні засоби захисту на кожен мобільний пристрій, перш ніж дозволити працівнику доступ до систем або інформації організації;
- регулярно оновлювати мобільні операційні системи та програми;
- регулярно проводити моніторинг та підтримку безпеки мобільних пристроїв;
- впровадити механізми ізоляції даних, наприклад, шифрування на основі особистого ключа працівника;
- встановити паролі на усі корпоративні пристрої та додатково посилити захист, впровадивши біометричні методи автентифікації.

Керівним методом посилення безпеки мобільних пристроїв є впровадження управління корпоративною мобільністю (EMM) – рішення, яке використовується для розгортання, налаштування та активного керування мобільними пристроями в корпоративному середовищі. За допомогою EMM у відділу кібербезпеки з’являється можливість встановити додаткові правила та обмеження для мобільних пристроїв, які підвищують їхню безпеку (табл. 3.1).

Таблиця 3.1 – додаткові заходи безпеки за ЕММ [17]

Механізм безпеки пристрою	Заходи
Розблокування	Вимагати пароль або біометричні дані для розблокування пристрою. Вимагати код доступу, токен, цифровий сертифікат або інші механізми автентифікації для доступу до інформації. Обмеження кількості невдалих спроб, після якої у розблокуванні пристрою чи доступі до інформації буде відмовлено.
Блокування	Автоматичне блокування пристрою після встановленого часу бездіяльності. Віддалене блокування пристрою, якщо є підозра у його втраті, крадіжці або в тому, що він був залишений розблокованим без нагляду.
Знімні носії	Введення в експлуатацію індивідуальних знімних носіїв, без яких неможливо отримати розшифрування зашифрованої інформації, коли такий носій не підключено до конкретного пристрою.
Видалення даних	Стирати дані з пристрою після визначеної кількості невдалих спроб доступу. Дозволити дистанційно стирати дані з пристрою у випадку його втрати чи викрадення. Повне стирання даних перед виведенням пристрою з обігу або передачею його наступному користувачу.
Синхронізація	Обмеження синхронізації пристроїв, веб-сайтів та програм.

Продовження таблиці 3.1.

Механізм безпеки пристрою	Заходи
Програми	Обмеження дозволених магазинів застосунків (наприклад, дозвіл завантаження програм лише із застосунку Google play або заборона встановлення будь-яких магазинів застосунків, крім цього). Обмеження дозволених програм через створення білого списку програм (див. розділ 3.1.3) або внесення певних програм до списку заборонених. Ведення актуального списку усіх програм, встановлених на пристрої. Використання лише офіційних застосунків організації. Введення обов'язкових політик, які застосовуються до усіх програм, навіть, якщо деякі з них не є власністю підприємства. Обмеження дозволів кожної програми (доступів до мікрофону, камери, місцезнаходження тощо).

У деяких організаціях дозволена політика використання власного пристрою для роботи (BYOD). При застосуванні подібної політики безпека використання значною мірою знижується, адже для них неможливо встановити постійний моніторинг і перевірку активності пристрою. Загалом захист таких пристроїв майже не відрізняється від наведених вище рекомендацій (без урахування EMM), однак можуть бути введені додаткові заходи безпеки. Розповсюдженим рішенням безпеки для таких пристроїв є введення корпоративного VPN, без увімкнення якого працівник не має можливості підключитися до робочої мережі та переглядати файли, обмінюватися інформацією тощо. Для таких мобільних пристроїв також є обов'язковим встановлення антивірусного ПЗ чи введення обмежень на дозволені для встановлення застосунки. За можливості рекомендовано застосовувати

двофакторну автентифікацію. Як і для корпоративних пристроїв, на особистих мобільних має бути обмежено сихронізацію із застосунками (наприклад, вимкнено дозволи на перегляд місцезнаходження, перегляд галереї тощо) [18].

Додатковим методом захисту для будь-якого типу пристроїв є навчання працівників для визначення фішингових атак, підозрілих програм або процесів на пристрої, визначення необхідності вчасного оновлення операційної системи.

3.1.2 Захист хостів

Основним методом захисту хостів мережі є контейнеризація – підхід до розробки програмного забезпечення, при якому застосунок або служба, їх залежності і конфігурація «упаковуються» разом в образ контейнера. Контейнерну програму можна протестувати і підготувати до використання. Процес «обгортання» програм у контейнери фактично призводить до створення придатної для використання версії програми, яка працює та готова відповідати на запити так само, як і оригінал. Коли образ запаковується в контейнер, він не змінюється, а натомість до контейнеру потрапляє його копія, яка перетворюється з неактивного набору коду програми на запущений екземпляр програми.

Коли програми в контейнерах потрібно оновити, існуючі контейнери не змінюються – вони знищуються, а нові контейнери створюються з оновлених образів. Це ключова операційна відмінність контейнерів: базове програмне забезпечення з початкового розгортання не змінюється з часом, а відбувається заміна всього образу одночасно. Такий підхід має потенційні переваги безпеки, оскільки дозволяє організаціям створювати, тестувати, перевіряти та розгортати програмне забезпечення, не змінюючи його характеристик та конфігурації на кожному етапі.

Після впровадження рішення контейнеризації організаціям рекомендовані наступні засоби посилення безпеки [19]:

- Використовувати лише контейнеро-орієнтовані ОС, які були розроблені спеціально для запуску та взаємодії лише з контейнерами застосунків. У деяких випадках доречним буде також відключення усіх інших служб і

додаткових функцій ОС, якщо вони не є необхідними для забезпечення функціонування контейнерів.

- Здійснювати сегментацію контейнерів за призначенням, вразливістю до атак чи рівнем критичності для організації. Кожен визначений сегмент має зберігатися на окремому ядрі операційної системи, щоб забезпечити «ізоляцію» різних категорій контейнерів одна від одної. Використовуючи такий метод розподілу можливо уникнути поширення кіберінциденту, що виник в одній групі, на іншу.
- Автоматизація виявлення та локалізації компрометацій, залишкових даних, тимчасових файлів та інших можливих підозрілих файлів чи процесів на кожному окремому ядрі локальної ОС.
- Використовувати інструменти та процеси управління безпекою контейнерів, наприклад, такі, як перевірка оновлень «оригіналів» програм, фактичний час запуску контейнеру, перевірка контейнера на наявність відомих вразливостей. Наступним кроком безпеки контейнерів може бути рішення безпеки, що є вбудованим у контейнер і яке може моніторити середовище контейнера та забезпечувати точне виявлення аномальної чи шкідливої активності в ньому.
- Введення «кореня довіри» – такого джерела даних, якому завжди можна довіряти. У випадку контейнеро-орієнтованої системи до такого кореня мають входити дані конфігурації та прошивки хоста. Якщо вимірювання, здійснені під час запуску хоста, збігаються зі збереженими у корені довіри – хосту можна довіряти. Пізніше такий ланцюг довіри, що базується на апаратному забезпеченні, може бути розширений на ядро ОС та її компоненти, щоб забезпечити криптографічну перевірку механізмів завантаження, образів системи, середовищ виконання контейнерів та образів контейнерів.

3.1.3 Створення білого списку програм

Білий список програм – це список таких програм і компонентів (бібліотек, файлів конфігурації тощо), яким дозволено бути активними та які дозволено встановлювати на хості на основі чітко визначених критеріїв.

Формування білого списку забезпечується на основі заздалегідь визначених файлових атрибутів «відбору», що були обрані організацією для запобігання запуску шкідливого програмного забезпечення та іншого несанкціонованого програмного забезпечення. На відміну від інших технологій безпеки, наприклад, таких як антивірусне програмне забезпечення, де використовуються чорні списки – вони блокують відомі шкідливі дії та програми і дозволяють виконання усіх інших. Технології білого списку програм розроблені для того, щоб дозволяти для запуску і роботи відомі безпечні процеси і програми та блокувати усі інші.

Як вже було вказано, білий список програм обов’язково формується на основі заздалегідь визначених файлових атрибутів, які можна аналізувати для виявлення заборонених програм чи процесів. Такими атрибутами можуть бути [20]:

- ім’я файлу;
- розмір файлу;
- шлях до файлу;
- електронний підпис;
- криптографічне геш-значення.

Зберігання криптографічних геш-значень дозволених програм є найбезпечнішим методом для створення білого списку – досягти непомітної зміни такого атрибуту вкрай важко, а також розмір гешу не буде залежати від шляху до файлу чи його назви. Єдиним важливим елементом для забезпечення надійності білого списку на основі гешів є регулярне оновлення інформації – у випадках внесення офіційних змін до програмних версій їх геш також буде змінюватись. Окрім цього, у випадку видалення застарілих гешів без відповідного призначення нових, значною мірою підвищиться ризик запуску шкідливого ПЗ.

Електронний підпис загалом не поступається надійністю криптографічному гешуванню, адже файл програми також отримує унікальне значення, яке додатково

підтверджує, що файл не було змінено і він є офіційним. Однак буває вкрай важко досягти використання лише таких програм на підприємстві, що були попередньо підписані електронним підписом постачальника, адже практика електронного підписання програм ще не набула широкого розповсюдження. Можливим варіантом функціонування такого білого списку є внесення підтвердження надавача послуг [20]. За такої ідентифікації користувачам організації будуть доступні усі програми від підтвердженого безпечного постачальника. Недолік цього варіанту полягає у тому, що тоді й старі версії програм або небажане програмне забезпечення від такого постачальника стане доступним до запуску, що може призвести до появи вразливостей у мережі.

Ім’я файлу, його розмір та розташування в свою чергу є більш «загальними» атрибутами. Їхнє використання рекомендується лише у випадку неможливості формування білого списку програм на основі розмірів гешу чи електронних підписів. Також рекомендується одночасне використання хоча б двох з трьох атрибутів для підвищення надійності визначення безпечності застосунку, так як розміри шкідливих файлів можуть відповідати розмірам дозволених до використання; назви файлів можуть змінюватися для відповідності назвам, зазначеним у списку; чи зловмисники можуть розміщувати шкідливі файли у папках за визначеним шляхом доступу.

Хоча зазвичай технологія білого списку програм не передбачає використання чорного списку, кожна організація може змінювати налаштування режимів роботи подібного рішення в залежності від поточних потреб і вимог захисту кібербезпеки. Можливими режимами роботи білого списку є аудит та примусове виконання.

При використанні режиму аудиту з технологіями білого списку до виконання дозволяються усі елементи, навіть такі, що не зареєстровані у списку. Виконання кожного програмного файлу обов'язково фіксується, а застосування цього режиму вимагає постійного моніторингу та аналізу активності.

Якщо ж для білого списку застосовується режим примусового виконання, то можливі три наступні сценарії робочого процесу [20]:

- до виконання допускаються лише файли, що містяться у білому списку, будь-які інші – блокуються;
- до виконання допускаються і такі файли, що не були внесені до білого списку, але система обов'язково запитує користувача щодо дозволу чи заборони запуску обраної програми;
- до виконання допускаються будь-які файли, незважаючи на білий список програм, якщо такі файли не були внесені до чорного списку.

3.1.4 Захист хмарних систем

Хмарні технології дозволяють зберігати інформацію не на локальних пристроях, а отримувати до неї доступ через віддалені сервери мережі. Розглядаючи цей підхід детальніше, можна виділити три сервіси, які можуть використовуватися із залученням хмарних послуг [21]:

- доступ до програмних застосунків, наприклад електронної пошти (модель обслуговування «програмне забезпечення як послуга», SaaS);
- середовище для створення та експлуатації власного програмного забезпечення (модель обслуговування «платформа як послуга», PaaS) або мережевий доступ до віртуалізованих обчислювальних систем;
- ресурси, наприклад, сховище для зберігання документів (модель обслуговування «інфраструктура як послуга», IaaS).

Для посилення безпеки послуг SaaS організації мають впровадити загальну політику користування, яка застосовуватиметься як для основного ПЗ, так і для його копій (реплік), які можуть знаходитися в інших країнах чи бути перекладені іншою мовою. Важливо враховувати, чи буде забезпечуватися синхронізація реплік з основним джерелом, а також надавати для усіх варіацій існуючого ПЗ вчасні оновлення політик безпеки і правил використання. Окрім забезпечення дотримання правил користування послугами, для SaaS необхідне впровадження управління привілеями, яке включає додавання, видалення та зміну привілеїв суб'єкта. Іншою ланкою контролю доступу є перевірка прав доступу користувачів – для багатокористувацького орендування обов’язково має бути введена авторизація.

Після забезпечення надійних методів надання доступу до програмних застосунків необхідно звернути увагу і на забезпечення цілісності, конфіденційності та доступності інформації, що розміщується на сервісі. Для цього організації можуть впровадити власні схеми шифрування, розшифрування яких можливе лише авторизованим користувачем. При впровадженні шифрування варто враховувати, що занадто складні методи значною мірою вплинуть на продуктивність мережі, через що необхідно додатково визначати оптимальне рішення із забезпеченням балансу показників захищеності і часу обробки інформації [21].

PaaS система дозволяє розробникам створювати власні застосунки у хмарних платформах, через що постають питання доступу користувачів між застосунками, фінансовими операціями та управлінням доступом до усіх можливих сервісів конкретного створюваного застосунку. Щоб розробка у PaaS була безпечною, необхідно забезпечити область дії застосунків так, щоб кожен окремий застосунок мав доступ лише до тих даних користувачів, які були введені у цьому застосунку. Крім цих заходів, для PaaS рекомендовано ввести централізовану архітектуру для забезпечення дотримання політик доступу, які б регулювали доступ до кожного використаного при розробці мікросервісу (наприклад, сервісу обробки транзакцій). Як вже було вказано для моделі обслуговування SaaS, використовувані сервіси та розроблені застосунки можуть бути реалізовані декількома мовами або перекладені пізніше, тому для кожної версії застосунку може знадобитися розробка власного механізму авторизації [21]. Організаціям також рекомендовано застосувати автоматичне очищення кеш-пам'яті процесора під час перемикання між застосунками для прискорення робочих процесів. Однак, повне очищення кешу може навпаки знизити продуктивність, тому частіше за все при використанні PaaS зупиняються на стиранні лише таких даних, які визначені підприємством як критично конфіденційні.

Щоб посилити кібербезпеку моделі обслуговування IaaS, необхідно забезпечувати більшість вищеописаних засобів захисту, адже при використанні такої моделі користувачі можуть як зберігати власні документи, застосунки,

унікальну інформацію забезпечення доступу, так і створювати нові багатокористувацькі документи, опитування і т.д. Подібна мережа постійно спільно використовується споживачами IaaS, через що необхідне введення контролю доступу до мережі, створення списків дозволених користувачів для з'єднання, блок-листів для користувачів та можливість розподіляти навантаження на систему з урахуванням кількості поточних підключень. Можливим необхідним заходом може бути введення рівнів доступу до мережі. Організація, що використовує рішення IaaS, має також забезпечити захист від витоку інформації, обмежуючи спільне використання ресурсів. В окремих випадках може знадобитися введення заборони на використання інформації з буферу обміну.

3.1.5 Правила безпечної розробки

Безпечна розробка – це набір практик, методів і процесів, інтегрованих на всіх етапах життєвого циклу розробки програмного забезпечення, які спрямовані на підвищення стійкості кінцевого продукту до кібератак.

У підрозділі 1.3 вже згадувалися деякі з методів безпечної розробки, зокрема використання ролей і привілеїв для користувачів та навчання персоналу. Ці методи здебільшого стосуються саме підготовки організації до застосування правил і вимог безпечної розробки. Також на етапі підготовки необхідно створити відповідну політику, у якій будуть зазначені вимоги щодо розробки програмного забезпечення.

Наступним етапом безпечної розробки буде забезпечення захисту програмного забезпечення: доступ до коду повинні мати лише працівники команди розробки або такі, що мають відповідні привілеї (рівні доступу). Необхідно впровадити безпечні репозиторії та автоматичне сканування середовища розробки. Окремо варто виділити процес рецензування коду, який є обов’язковим для перевірки на вразливі чи недостатньо оброблені ділянки майбутнього ПЗ. Після завершення розробки програмного забезпечення (або також у процесі написання коду) критично важливим є створення тестових сценаріїв, за якими можна перевірити процес роботи застосунку. Доречним буде застосування модельованих

атак на ПЗ (пентестів, penetration testing) для перевірки стійкості розробленого забезпечення.

Після успішного впровадження розробленого ПЗ необхідно створити політику реагування на кіберінциденти і канал звітування про події безпеки. Особливості реагування на інциденти безпеки були описані у підрозділі 1.2. Обов’язковим є також визначення пріоритетності кіберінцидентів, усі можливі варіації якого вже були представлені у розділі 2.

Ще одним раніше згаданим рішенням для безпечної розробки є впровадження ZTA – такий підхід до кібербезпеки виключає можливість неавторизованих підключень, постійно перевіряє та аналізує усі дії користувачів і потоки трафіку, а також вимагає використання політик безпеки для кожної існуючої частини середовища.

3.2 MITRE ATT&K

Для швидкого виявлення кіберінцидентів організаціям рекомендовано користуватися базами даних щодо вразливостей, експлойтів та інших можливих загроз комп'ютерній безпеці. Як було описано раніше, на сьогоднішній день існує великий вибір подібних інструментів – наприклад, національна база даних вразливостей, бази даних від CERT-UA (або CERT/CC) та MITRE ATT&K.

Найбільш оптимальним методом буде використання одразу декількох баз даних, однак, реалізувати автоматизоване усунення або швидку оцінку командою реагування на інциденти за такого сценарію буде вкрай важко, адже додатковий час буде витрачатися на аналіз кожного з представлених ресурсів. Відтак, організаціям потрібно обирати провідне джерело інформації стосовно кіберінцидентів, вразливостей, нових шкідливих програм та інших можливих загроз.

Хоча дуже критичних відмінностей між актуальними базами даних зазвичай немає, для імплементації організаціями рекомендується використання MITRE ATT&K.

MITRE розробила ATT&CK у 2013 році для документування тактик, технік та процедур (ТТП), які зловмисники використовували для цілеспрямованих

кібератак на корпоративні інфраструктури під керуванням операційної системи Windows. Наразі ATT&CK є базою даних стосовно кібератак і системою класифікацій дій зловмисників та у ній міститься опис шкідливих дій, спрямованих проти одразу кількох видів інфраструктур [22]. Для зручної орієнтації на офіційному сайті MITRE база даних додатково розподіляється на матриці, які містять інформацію стосовно ТТП для конкретних інфраструктур [23]. Наприклад, на рис. 3.2 представлено матрицю для корпоративних інфраструктур.

Рисунок 3.2 – Матриця ТТП для корпоративних інфраструктур

З часом можливості застосування ATT&CK розширювалися, та на сьогоднішній день її можна використовувати для:

- корпоративних інфраструктур під керуванням Windows, MacOS та Linux;
- мережевих пристроїв та технологій контейнерної віртуалізації;
- хмарних середовищ, таких як IaaS, SaaS, Office 365, Azure Active Directory (Azure AD) та Google Workspace;
- пристроїв промислових мереж;
- серверів управління та архівних даних;
- інженерних робочих станцій;
- серверів введення та виводу;
- систем і терміналів протиаварійного захисту;

- мобільних пристроїв під керуванням Android та iOS.

ATT&CK є відкритою і безкоштовною для користування як для окремого користувача, так і для цілих підприємств. Її можна використовувати для підтримки різних процесів забезпечення захищеності, розвитку архітектури безпеки, дослідження кіберзагроз тощо. Оновлення бази даних відбувається двічі на рік.

MITRE ATT&CK не є програмним забезпеченням як таким. Але багато корпоративних програмних рішень для безпеки, таких як аналітика поведінки користувачів та об’єктів (UEBA), розширене виявлення та реагування, оркестрація безпеки, автоматизація та реагування (SOAR) та управління інформацією та подіями безпеки (SIEM) – можуть інтегрувати інформацію про загрози MITRE ATT&CK для оновлення та покращення своїх можливостей виявлення та реагування на загрози.

3.3 Обмін інформацією про кіберінциденти

У деяких випадках виникають вимоги до обміну інформацією з третіми сторонами або поширення інформації про кіберінцидент «на загал». Наприклад, організації може знадобитися досвід іншого підприємства стосовно управління кіберінцидентами, або вплив кіберінциденту розповсюдився за межі організації (стався виток особистих даних клієнтів, виток баз даних стосовно фінансових активів організації тощо). Як вже було визначено у розділі 2, за високої критичності кіберінциденту може також з’явитися необхідність у зверненні до Національної поліції, СБУ чи інших правоохоронних органів. На рис. 3.4 зазначені усі можливі комунікації при обміні інформацією.

Відтак, постає питання правильного обміну інформацією, щоб запобігти надмірного поширення конфіденційних даних або її витоку до таких третіх осіб, дозвіл на ознайомлення яким не було надано.

Незалежно від терміновості обміну інформацією, процес зазвичай відбувається за наступною послідовністю (рис. 3.3):

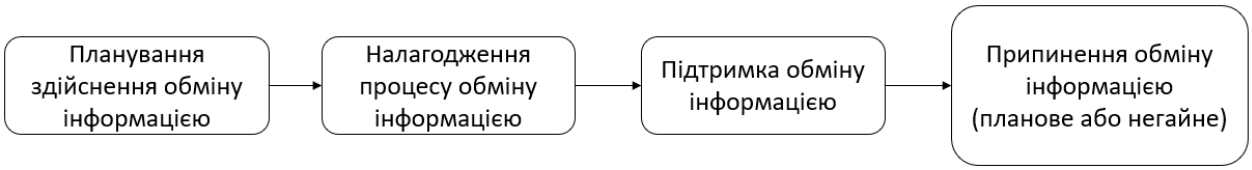

Рисунок 3.3 – Процес обміну інформацією

Передумовами для захищеного та якісного обміну інформацією є [24]:

- Встановлення цілей та завдань обміну інформацією, які сприяють розвитку кібезпеки організації, збагаченню її знань і методів протидії кіберінцидентам.
- Створення опису усіх існуючих в організації загроз безпеці інформації, вже реалізованих атак на мережу, особливостей функціонування компонентів та «слабких місць» безпеки даних. Додатково організація має визначити, які з описаних загроз і ризиків є дозволеними до розголошення під час обміну інформацією.
- Визначити тип та обсяг інформації, яка може надаватися при комунікації за межами власної команди реагування, а також зазначити обставини, за яких обмін такою інформацією є прийнятним.
- Визначити сторонні команди реагування, підприємства, постачальників та інших можливих сторін, з якими дозволений обмін інформацією.
- Встановити правила обміну інформацією, які враховують надійність одержувача, конфіденційність обмінюваної інформації та потенційний вплив обміну (або нерозповсюдження) певних типів інформації.
- Долучатися до публічних заходів обміну інформацією, наприклад, наукових конференцій чи веб-сайтів інших компаній.
- Введення індикаторів дозволу для інформації (маркування конфіденційної інформації TLP, Traffic Light Protocol).
- Введення в експлуатацію лише безпечних протестованих процесів автоматизації, використання, аналізу та реагування на інформацію про кіберзагрози.

- Заздалегідь укладати угоди стосовно розповсюдження інформації, які будуть визначати правила і вимоги щодо обміну даними між усіма організаціями-учасницями (або усіма командами).
- Ведення документації стосовно здійснених обмінів інформацією, власних зібраних даних стосовно кіберінцидентів та інших загроз безпеці, інформації стосовно наявних у мережі вразливостей та впроваджених засобах її пом'якшення чи усунення.

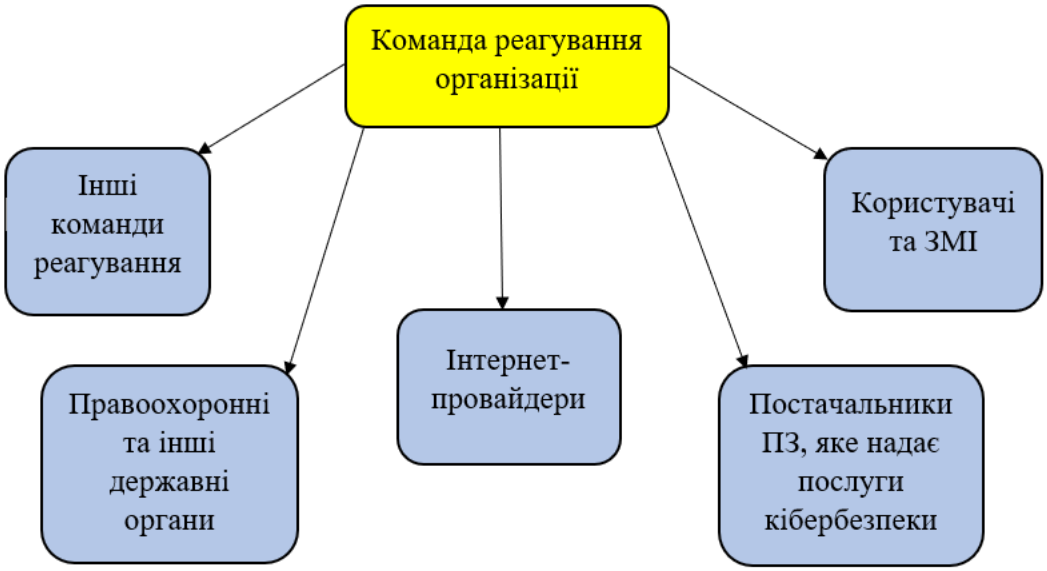

Рисунок 3.4 – Можливі комунікації при обміні інформацією

Іноді можуть виникати надзвичайні ситуації, які вимагають негайного обміну інформацією. Для таких ситуацій може не існувати створених угод або не вистачати часу для дотримання усіх встановлених правил і вимог обміну інформацією. У таких випадках організаціям рекомендовано використовувати вже існуючі угоди стосовно нерозголошення інформації та дотримуватись принципів надання дозволів доступу, які вже були впроваджені до виникнення надзвичайної ситуації [25]. Організація-власник інформації також зобов'язана вести документацію інформації, обмін якою було здійснено під час врегулювання ситуації, обґрунтувати доцільність і необхідність її обміну та задокументувати усіх осіб, які брали участь в обробці надзвичайної ситуації, з призначеними їм ролями.

Для швидкого визначення, чи може інформація бути розголошеною, зручно використовувати маркування TLP, згадане вище. TLP визначає обмеження щодо інформації, керуючись правилом світлофора: для найбільш конфіденційної інформації, яка не може розголошуватись поза межами певної зустрічі, застосовується червоний колір, відповідно до менш обмежених для обміну типів інформації визначаються жовтий і зелений кольори (табл. 3.2) [26].

Таблиця 3.2 – Маркування конфіденційної інформації

Колір	Обмеження
Червоний	Конфіденційна інформація, заборонена до розповсюдження будь-де, окрім зустрічі або розмови, де вона була вперше використана.
Жовтий	Інформація може бути поширена лише в межах організації чи таких ситуаціях, коли нерозголошення може призвести до критичних наслідків для користувачів або клієнтів.
Зелений	Інформація може бути поширена між іншими командами реагування, організаціями-колегами тощо, але має передаватися захищеними каналами.
Білий	Інформація може бути поширена у будь-якому вигляді без обмежень.

Окрім вже описаних процедур обміну, буває необхідним публічне поширення інформації. Розкриття інформації у ЗМІ здійснюється, якщо [27]:

- кіберінцидент є новим або вкрай рідкісним, через що його не було внесено до баз даних і не існує створених правил для його нейтралізації;
- усунути вразливість не вдалося, і користувачам наразі доступна лише така версія застосунку/системи/тощо;
- існує ризик витоку конфіденційної інформації, наприклад, особистих даних користувачів;
- користувачам необхідно терміново встановити оновлення, іншу версію застосунку чи змінити пароль, щоб уникнути небезпеки;

- виявлена вразливість стосується програмного коду застосунку, сайту тощо.

Якщо ж поява вразливості спричинена використанням відкритого коду для проєктування застосунку, сайту, програмного забезпечення тощо, то має бути створено офіційне публічне попередження щодо можливих вразливостей, пов’язаних з його використанням.

3.4 Відновлення після кіберінциденту

Обов'язковою подією після усунення кіберінциденту є відновлення уражених активів, робочих процесів та інших ресурсів організації. Швидке відновлення дозволяє максимально зберегти продуктивність роботи підприємства та його репутацію серед користувачів, що робить його критично важливим етапом циклу обробки інцидентів безпеки.

Для забезпечення злагодженого відновлення організація має створити і розповсюдити серед працівників наступні документи [28]:

- план відновлення із переліком чітких інструкцій дій у разі виникнення кіберінциденту, пріоритезації захисту активів, процедур керування доступом та цілей відновлення;
- схематичне уявлення (план) робочої системи із вказанням додаткових особливостей її функціонування, якщо такі наявні;
- задокументована інфраструктура мережі, правила доступу до неї та перелік усіх апаратних і програмних ресурсів організації із вказанням особливостей обробки інформації в них;
- задокументовані резервні ресурси, що можуть бути введені в тимчасову експлуатацію у випадку відмови основних ресурсів або містять копії даних, з яких можна відновити ушкоджені оригінали;
- опис документів та активів, друковані та матеріальні копії яких зберігаються;
- контактна інформація працівників, відповідальних за реалізацію плану;
- контактна інформація усіх членів команди реагування на події безпеки;

- задокументований максимально допустимий час простою, погіршення пропускної здатності та інших можливих негативних впливів;
- план робочого процесу у разі неможливості відновлення протягом визначеного допустимого часу простою;
- план комунікації у разі компрометації каналу зв'язку, необхідності залучення інших організацій чи необхідності розкриття інформації про кіберінцидент (для офіційних звітностей, застереження користувачів ураженої мережі тощо).

Планування відновлення включає розробку процесів та процедур, які є достатньо гнучкими, щоб забезпечити своєчасне відновлення систем та інших активів, постраждалих від можливих кіберінцидентів, а також достатньо комплексними, щоб мати модульні компоненти для часто використовуваних процедур, наприклад, таких як відновлення контролю над обліковими записами [28]. На цьому етапі також необхідно створити документ – керівництво або посібник відновлення, де будуть поетапно зазначені усі необхідні процедури і технічні процеси, які очікуються до виконання під час процесу відновлення та засоби автоматизації таких процедур і процесів.

На основі вищезазначеної документації (плану відновлення, списку ресурсів тощо) команда, що займається відновленням, має визначити конкретні засоби відновлення, релевантні до виниклого кіберінциденту, а також визначити подальшу стратегію відновлення і комунікації після усунення інциденту. При визначенні дій щодо усунення інциденту кібербезпеки має враховуватися його рівень критичності та рівень критичності ураженого активу.

Ефективне відновлення включатиме постійне використання та вдосконалення як технічних, так і нетехнічних заходів. Для швидкого виявлення несприятливих подій потрібне впровадження постійного моніторингу подій, перевірки прав доступу користувачів, аналізу сертифікатів та інших ресурсів і процесів організації. Щоб виявити неточності у сценаріях реагування та відновлення, а також недостатню обізнаність працівників щодо дій у разі виникнення кіберінцидентів, доцільно буде впровадити періодичне тестування

розроблених послідовностей дій та програмних засобів з їхньої автоматизації. Навіть після контрольованого моделювання подій безпеки рекомендовано складати звіт виконаних дій та досягнутих результатів.

Важливо зазначити, що відновлення має відбуватися лише за умови, коли кіберінцидент було повністю оброблено, а зловмисника – вилучено з мережі. Дієздатність відновлення завжди оцінюється за можливістю визначення початкової цілі зловмисника та визначення методів і засобів, що були ним використані. Критично важливо не розповсюджувати інформацію щодо визначених цілей та методів до завершення розслідування, адже існує ризик компрометації, при якому зловмисник зможе бачити дії команди реагування та змінювати тактики атаки.

ВИСНОВКИ

Визначення рівнів критичності кіберінцидентів є необхідним для організацій будь-яких розмірів, адже воно:

- дозволяє зменшити час, необхідний на виявлення, обробку та відновлення після кіберінциденту;
- дозволяє ефективно розподіляти ресурси при реагуванні на інцидент безпеки;
- пропонує значне прискорення вибору заходів обмеження дії кібератак;
- допомагає зменшити фінансові та матеріальні втрати за рахунок вчасного реагування на несприятливі події безпеки.

Існує великий вибір методів визначення критичності кіберінцидентів, однак не всі з них є актуальними і ефективними для використання. У результаті дослідження методів та їхнього порівняльного аналізу було визначено, що переваги у швидкості і точності визначення інцидентів безпеки мають такі варіанти пріорітезації, які дозволяють впровадження автоматизації заходів реагування та пропонують користувачам кількісну оцінку на основі одразу декількох характеристик. Введення додаткових метрик та характеристик (наприклад, як у міжнародному стандарті CVSS) також забезпечує високу об’єктивність кінцевої оцінки.

Для кіберпростроpу України було сформовано модель реагування на основі рівнів критичності кіберінцидентів, які були визначені на державному рівні Адміністрацією Держспецзв’язку.

Важливим етапом роботи також було висвітлення можливостей захисту від кіберінцидентів, обміну інформацією щодо них та визначення правильної послідовності дій для відновлення після інцидентів.

Обов’язковим для використання протоколом під час обміну інформації є TLP, що розподіляє інформацію за «кольором доступу» – навіть за надзвичайної події, коли немає часу на формування правил та обов’язків обміну інформацією між

сторонами, такий підхід дозволяє швидко орієнтуватись у рівнях конфіденційності даних організації.

У результаті роботи було досягнуто мети – було узагальнено наявні відомості про методи пріорітезації кіберінцидентів та визначено правильний алгоритм дій реагування у разі виявлення кіберінцидентів. Дослідження забезпечило доступність інформації щодо засобів і методів захисту кіберпростору від можливих інцидентів безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Morris worm. 2025. Режим доступу: https://en.wikipedia.org/wiki/Morris_worm
2. NIST Special Publication 800-61 Rev. 2. Computer Security Incident Handling Guide. 2012. Режим доступу: https://csrc.nist.gov/pubs/sp/800/61/r2/final.
3. Відкрита база даних загроз. Режим доступу: https://github.com/VISWESWARAN1998/open-threat-database/tree/master (дата звернення 15.11.2025).
4. CISA Посібник з додаткових ресурсів CRR Том 5 Управління кіберінцидентами. 2016. 54 с.
5. Наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570 «Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі». Режим доступу: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori.
6. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. 2020. Режим доступу: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.
7. NIST Special Publication 800-207 Zero Trust Architecture. 2020. Режим доступу: https://csrc.nist.gov/pubs/sp/800/207/final.
8. Shackleford D. Who's Using Cyberthreat Intelligence and How? SANS Institute. 2015. 24 с.
9. Brown S., Lee R The Evolution of Cyber Threat Intelligence (CTI) SANS Institute. 2019. 16 с.
10. ENISA (European Union Agency for Cybersecurity) Good Practice Guide on Incident Management. 2020. 110 с.

11. Friedberg I., Skopik F., Settanni G., Fiedler R. Combating advanced persistent threats: From network event correlation to incident detection Computers & Security. 2017. 23 с.
12. Системи аналізу поведінки користувачів та сутностей (User and Entity Behavior Analytics – UEBA). Режим доступу: https://eska.global/solutions/ueba (дата звернення 20.11.2025).
13. Базові метрики Загальної системи оцінки вразливостей версії 3.1 Common Vulnerability Scoring System version 3.1: Specification Document. Режим доступу: https://www.first.org/cvss/v3.1/specification-document (дата звернення 25.11.2025).
14. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.05.2023 № 463 «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами». Режим доступу: https://zakon.rada.gov.ua/rada/show/v0463519-23#Text.
15. Покроковий процес пріоритизації за CISA. 2021. Режим доступу: https://www.cisa.gov/sites/default/files/2024-03/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.
16. Постанова Кабінету Міністрів України від 04.04.2023 № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі». Режим доступу: https://zakon.rada.gov.ua/laws/show/299-2023-п.
17. NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise. 2023. Режим доступу: https://csrc.nist.gov/pubs/sp/800/124/r2/final.
18. NIST Special Publication 1800-22 Mobile Device Security: Bring Your Own Device (BYOD). 2023. Режим доступу: https://csrc.nist.gov/pubs/sp/1800/22/final.

19. NIST Special Publication 800-190 Application Container Security Guide. 2017. Режим доступу: https://csrc.nist.gov/pubs/sp/800/190/final.
20. NIST Special Publication 800-167. Guide to Application Whitelisting. 2015. Режим доступу: https://csrc.nist.gov/pubs/sp/800/167/final.
21. NIST Special Publication 800-210. General Access Control Guidance for Cloud Systems. 2020. Режим доступу: https://csrc.nist.gov/pubs/sp/800/210/final.
22. Бази знань і додатки виявлення кіберінцидентів MITRE ATT&CK Framework. Режим доступу: https://www.mitre.org/focus-areas/cybersecurity/mitre-attack (дата звернення 20.11.2025).
23. Основні компоненти MITRE ATT&CK Framework/ATT&CK Matrix for Enterprise. Режим доступу: https://attack.mitre.org/ (дата звернення 20.11.2025).
24. NIST Special Publication 800-47 Rev. 1. Managing the Security of Information Exchanges. 2021. Режим доступу: https://csrc.nist.gov/pubs/sp/800/47/r1/final.
25. NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems. 2010. Режим доступу: https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final.
26. NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing. 2016. Режим доступу: https://csrc.nist.gov/pubs/sp/800/150/final.
27. NIST Special Publication 800-210 Recommendations for Federal Vulnerability Disclosure Guidelines. 2023. Режим доступу: https://csrc.nist.gov/pubs/sp/800/216/final.
28. NIST Special Publication 800-184 Guide for Cybersecurity Event Recovery. 2016. Режим доступу: https://csrc.nist.gov/pubs/sp/800/184/final.