DOI: 10.51369/2707-7276-2025-1(38)-6
УДК 004.056(045)

ВАВІЛЕНКОВА Анастасія Ігорівна
ORCID ID: 0000-0002-9630-4951

ПРОЦЕС УПРАВЛІННЯ КІБЕРІНЦИДЕНТАМИ ЯК НЕОБХІДНИЙ ЕТАП В ОРГАНІЗАЦІЇ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

У статті досліджено основні кроки процесу управління кіберінцидентами, проаналізовано особливості їхньої організації та визначено місце процесу управління кіберінцидентами в організації кібербезпеки підприємств. Це дає можливість правильно визначити пріоритети під час створення плану реагування та управління кіберінцидентами задля зменшення часу відновлення систем.

Детально описано кожен етап процесу управління кіберінцидентами як подіями навмисного або ненавмисного характеру, що становлять загрозу безпеці інформаційних систем або мереж і можуть призвести до порушення їхнього нормального функціонування.

Процес управління кіберінцидентами, що є невід'ємною частиною загальної стратегії кібербезпеки підприємств, розглянуто як систему, яка передбачає виявлення, аналіз, реагування та усунення наслідків деструктивних подій. Перший етап процесу управління кіберінцидентами – виявлення подій, під якими розуміють певні ситуації, які можуть порушити типову діяльність організації. Другий – сортування та аналіз подій, тобто класифікація потенційних кіберінцидентів, визначення пріоритету їх усунення. Третій етап – це відповідь та відновлення, тобто реагування на інцидент, обмеження впливу кіберінциденту, мінімізація шкоди від його настання. Четвертий – поліпшення можливостей, тобто відновлення нормальної роботи системи після локалізації та знешкодження кіберінциденту.

Зроблено висновок, що для забезпечення ефективної кібербезпеки підприємства повинні системно здійснюватися: оцінювання ризиків, розроблення політик і процедур безпеки, використання сучасних технологій для захисту інформаційних систем, навчання персоналу та створення плану управління кіберінцидентами.

Ключові слова: *виявлення подій, кібербезпека, кіберінцидент, кіберзагроза, реагування на кіберінциденти, управління кіберінцидентами.*

Постановка проблеми. Управління кіберінцидентами є важливою складовою кібербезпеки, оскільки допомагає організаціям швидко реагувати на загрози та мінімізувати шкоду від інцидентів, що можуть вплинути на інформаційні системи, дані, ресурси та репутацію організації. Заходи з організації кібербезпеки на підприємстві передбачають застосування сукупності методів і практик захисту інформаційної інфраструктури, докладання

постійних зусиль щодо захисту комп'ютерних мереж і систем, а також даних від несанкціонованого використання або пошкодження [1].

Основними цілями кібербезпеки є [2]:

– захист конфіденційних даних (організація політики безпеки щодо доступу до інформації, запобігання витоку інформації та несанкціонованому використанню даних, а також захист особистих даних працівників компаній);

– забезпечення цілісності інформації (запобігання фальсифікації даних, проникненню шкідливого програмного забезпечення, зміненню або пошкодженню даних під час зберігання або передавання);

– забезпечення доступності інформації (гарантування безперебійної роботи в реальному часі, доступність для користувачів, убезпечення від кібератак і забезпечення основних функцій критично важливої інфраструктури).

В умовах сучасного цифрового світу кіберінциденти можуть виникати будь-коли і в будь-якій організації, тому основною проблемою під час настання кіберінцидентів є необхідність розуміння не тільки того, що робити в разі їх виникнення, але й як підготуватися до їхнього ймовірного настання, створивши ефективний процес управління кіберінцидентами.

Аналіз останніх досліджень і публікацій. За даними оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України [3], за 2023 рік було опрацьовано 148 тисяч потенційних кіберінцидентів, що на 62,5 % більше, ніж у 2022 році.

Лише порівнюючи статистику результатів роботи кіберфахівців ситуаційного центру забезпечення кібербезпеки Служби безпеки України за десять та одинадцять місяців 2024 року [4], можна визначити, що кількість припинених атак за місяць становила 259, серед них 55 – у режимі реального часу. Також зі статистики виявлення та запобігання кіберінцидентам і кібератакам в Україні за січень–листопад 2024 року бачимо, що найчастіше атакам піддається сектор державної влади та транспорту, також фінансовий сектор, а основними типами загроз є спроби експлуатації вразливостей та використання шкідливого програмного забезпечення (див. рис. 1).

В Україні у складі Державної служби спеціального зв'язку та захисту інформації України існує спеціальна Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA [5], основними завданнями якої є ведення державного реєстру кіберінцидентів, надання допомоги щодо запобігання, виявлення та усунення наслідків кіберінцидентів, розроблення рекомендацій із питань протидії кіберзагрозам, проведення заходів з інформування щодо кіберзахисту, взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти й опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту. Також рішенням Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України затверджені загальні правила обміну інфор-

мацією про кіберінциденти [6]. Ці правила відповідають рекомендаціям Європейської агенції з кібербезпеки ENISA [7] та документу Форуму команд реагування та безпеки. З метою впровадження єдиної таксонометрії кіберінцидентів для ефективного обміну інформацією, швидкого розуміння, яких заходів необхідно вживати для реагування на той чи інший вид кіберінциденту, а також вчасного запобігання кіберзагрозам створено перелік категорій кіберінцидентів [8]. Аналіз низки джерел із проблематики, що розглядається, довів, що кількість заходів, які проводяться як в Україні, так і цілому світі щодо виявлення, реагування та запобігання кіберінцидентам, свідчить про те, що управління кіберінцидентами – це одна з найважливіших процедур управління інформаційною безпекою.

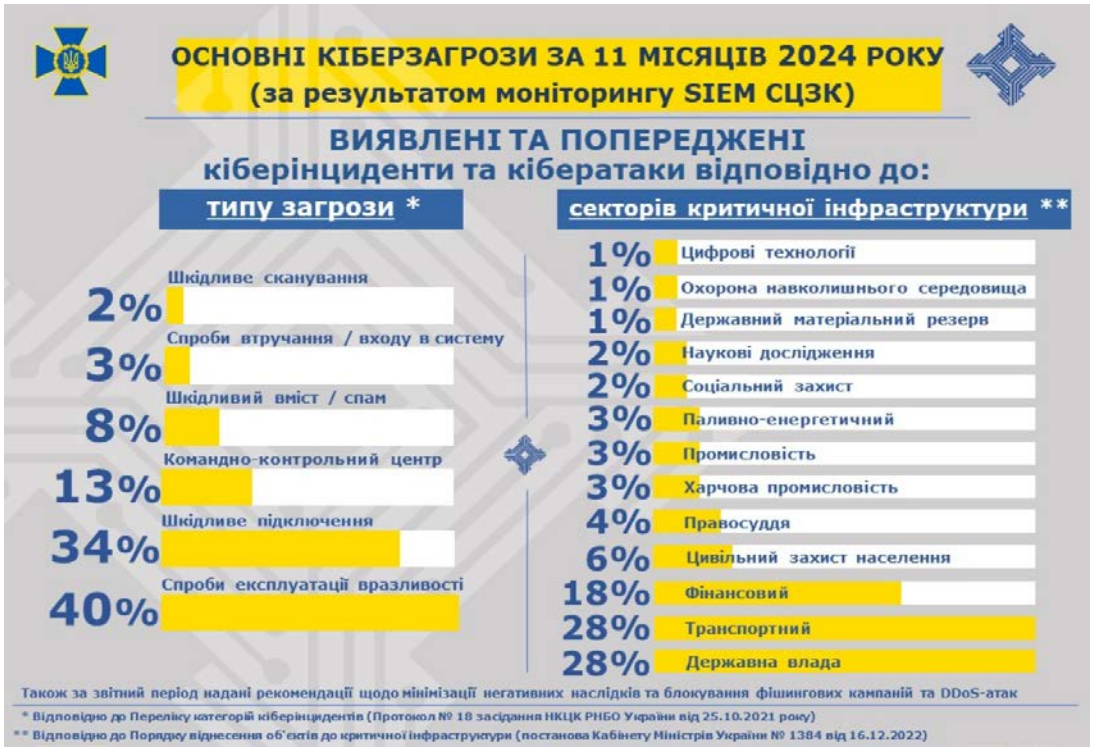

Рисунок 1 – Статистика виявлення та запобігання кіберінцидентам і кібератакам в Україні за січень–листопад 2024 року

Мета – дослідити основні кроки процесу управління кіберінцидентами, проаналізувати особливості їхньої організації та визначити місце процесу управління кіберінцидентами в процесі організації кібербезпеки підприємства. Це дасть можливість правильно визначити пріоритети під час створення плану реагування та управління кіберінцидентами задля зменшення часу відновлення систем.

Виклад основного матеріалу. Кіберінцидент – це подія навмисного або ненавмисного характеру, яка ста-

новить загрозу безпеці інформаційних систем або мереж і може призвести до порушення їхнього нормального функціонування [9]. Також кіберінцидентом можна назвати будь-яку подію в інформаційній системі або мережі, яка може призвести до порушення конфіденційності, цілісності або доступності даних чи інформаційних систем. Відповідно процес управління кіберінцидентами передбачає виявлення, аналіз, реагування та усунення наслідків деструктивних подій (див. рис. 2) [10]. Оскільки всі перераховані етапи спрямовані на запобігання несанкціонованому доступу до систем, виявлення зловмисного програмного забезпечення, запобігання атакам на мережі, витоку конфіденційних даних, фіксацію та усунення фізичних чи логічних порушень у роботі інформаційної інфраструктури, а відповідно є досягненням усіх основних цілей кібербезпеки, то можна вважати, що управління кіберінцидентами і є необхідним етапом в організації кібербезпеки підприємства. Розглянемо процес управління кіберінцидентами детальніше з метою визначення особливостей його реалізації під час організації заходів із кібербезпеки на підприємствах.

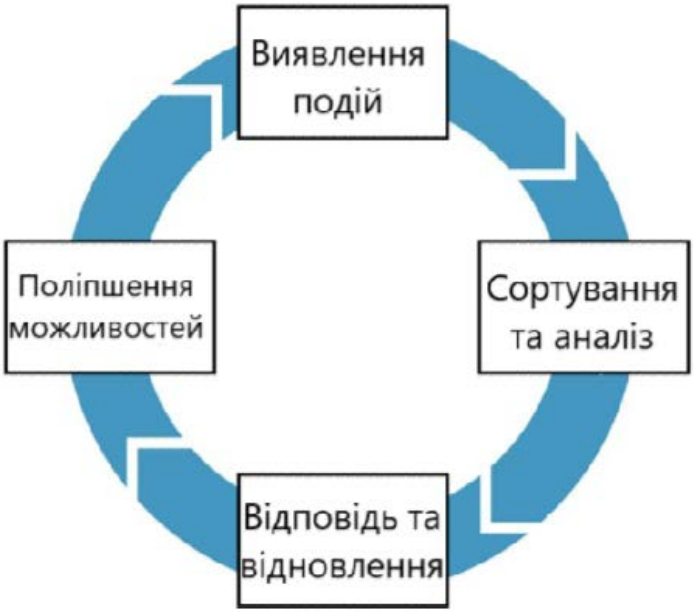

Рисунок 2 – Процес управління кіберінцидентами

Першим етапом процесу управління кіберінцидентами є виявлення подій, під якими розуміють певні ситуації, які можуть порушити типову діяльність організації. Зокрема до ознак кіберінцидентів належать [11]:

– порушення вимог конфіденційності – це отримання несанкціонованого доступу до інформації, втрата носіїв інформації, спроби отримати доступ вище наданого рівня, спроби зламу системи;

– порушення вимог цілісності – це виявлення вірусів та іншого шкідливого програмного забезпечення, пошкоджених секторів на жорстких дисках, помилок; спливаючі повідомлення, втрата даних або незаконні транзакції;

– порушення вимог доступності – це припинення роботи системи протягом неприйнятного періоду часу, фізична крадіжка пристроїв зберігання інформації, тривале перебування комп'ютерних вірусів в інформаційній інфраструктурі.

На першому етапі аналітики безпеки або співробітники підприємства можуть помітити нетипову роботу пристроїв, наприклад, повільну роботу персонального комп'ютера, часте самовільне перезавантаження, появу або зникнення повідомлень чи файлів, самостійне вимкнення антивіруса. Також можлива неавторизована спроба доступу до облікових записів, що виявляється через процес налаштування двофакторної автентифікації, або навпаки блокування процесу автентифікації через роботу під цим же акаунтом на іншому пристрої. Усе вказане вище є ознаками потенційних кіберзагроз. Саме тому важливими заходами на першому етапі управління кіберінцидентами є виявлення подій, їх фіксація, правильний опис та звітування, реєстрація виявлених подій у базі даних кіберінцидентів, відстеження статусу подій і подальша обробка даних відповідно до встановлених політик безпеки на підприємстві.

Другим етапом у процесі управління кіберінцидентами є сортування та аналіз подій, тобто класифікація потенційних кіберінцидентів, визначення пріоритету їх усунення.

Залежно від характеру та масштабів кіберінциденти можуть бути класифіковані так:

1) інциденти низької важливості – мінімальний вплив на систему, який не призводить до серйозних наслідків;

2) серйозні інциденти – інциденти, які суттєво впливають на функціонування системи або можуть спричинити витоки конфіденційних даних;

3) критичні інциденти – інциденти, що мають великий масштаб і можуть призвести до значних фінансових або репутаційних втрат для організації.

Для своєчасного реагування на кіберінциденти класифікація та пріоритезація кіберінцидентів повинні бути прописані завчасно у плані управління кіберінцидентами організації (див. рис. 3).

Для кожного типу інцидентів можуть бути різні підходи до їх виявлення, аналізу та реагування, тому важливо визначити серйозність інциденту та його впливу на процеси в роботі організації, ідентифікувати джерела загрози, якими можуть бути як зовнішні зловмисники, так і внутрішні працівники, а також визначити можливість порушення законодавства, втрати клієнтських даних або зупинки критично важливих процесів на підприємстві.

Третім етапом у процесі управління кіберінцидентами є відповідь та відновлення, тобто реагування на інцидент, обмеження впливу кіберінциденту, мінімізація шкоди від настання події. Реагування на кіберінциденти – важлива складова стратегії кібербез-

пеки підприємства, критична для збереження цілісності інформаційних систем, захисту конфіденційних даних, запобігання фінансовим втратам і забезпечення безперебійної роботи організації. Тому організація чіткої, послідовної та оперативної стратегії реагування на кіберінциденти стає необхідною умовою для успішного функціонування будь-якої сучасної інфраструктури.

Визначення пріоритету залежно від впливу та терміновості інциденту

		Вплив		
		Високий	Середній	Низький
Терміновість	Висока	1	2	3
	Середня	2	3	4
	Низька	3	4	5

Визначення часу для вирішення інциденту залежно від пріоритету

Пріоритет	Характеристика	Час вирішення
1	Критичний	1 год
2	Високий	8 год
3	Середній	24 год
4	Низький	48 год
5	Планується	Запланувати

Рисунок 3 – Приклад частини плану управління кіберінцидентами для визначення пріоритету кіберінцидентів

До заходів реагування на кіберінциденти належать:

1) відключення або ізоляція пошкоджених систем від основної інфраструктури, щоб уникнути подальшого поширення загрози;

2) проведення цифрового слідства для фіксації фактів інциденту, що може бути корисним у подальшому розслідуванні;

3) вживання заходів щодо усунення вразливості, якщо інцидент стався саме через уразливість системи.

Також важливими для відновлення є розроблення та реалізація заходів реагування, інформування зацікавлених сторін про кіберінцидент, повідомлення про статус події та відстеження кіберінцидентів.

Четвертим етапом у процесі управління кіберінцидентами є поліпшення можливостей, тобто відновлення нормальної роботи системи після локалізації та знешкодження кіберінциденту. Це передбачає організацію можливості:

– відновлення даних із резервних копій;

– виправлення програмних та апаратних помилок, які призвели до кіберінциденту;

– оновлення систем безпеки для запобігання повторному вторгненню;

– реалізація процесу постійного тестування програмного й апаратного

забезпечення на предмет виникнення вразливостей.

Після інциденту важливо провести аналіз для того, щоб визначити причини його виникнення та можливі шляхи покращання процесів безпеки в майбутньому. Зокрема важливими є постінцидентний аналіз для вивчення причин і результатів, розроблення нових політик безпеки на основі уроків, отриманих під час інциденту, проведення навчань і тренувань співробітників з метою підвищення їхньої обізнаності щодо кібербезпеки.

Висновки. Реагування на кіберінциденти є невід'ємною частиною загальної стратегії кібербезпеки підприємства. Система ефективного реагування включає чіткі етапи, починаючи з виявлення інциденту й завершуючи відновленням і підвищенням готовності організації до майбутніх загроз. Залежно від типу інциденту заходи реагування можуть бути різними, проте важливо, щоби процес був організованим і відпрацьованим для забезпечення мінімальних втрат. Постійний моніторинг, навчання персоналу та вдосконалення політик безпеки допомагають знизити ризики та підвищити стійкість підприємства до кіберзагроз.

Також ефективне управління кіберінцидентами потребує наявності на підприємстві добре організованої команди, у складі якої є різні фахові групи:

– керівник або менеджер інциденту, який відповідає за загальне управління інцидентом, координацію дій груп і підтримку зв'язку з вищим керівництвом;

– IT та безпекові спеціалісти, які працюють над технічними аспектами реагування та відновлення;

– юристи та фахівці з регулювання, які допомагають вирішувати питання правових наслідків інциденту, дотримання нормативних вимог і захисту репутації;

– спеціалісти з комунікацій, котрі займаються взаємодією з внутрішніми та зовнішніми зацікавленими сторонами, включаючи клієнтів, партнерів і регуляторні органи.

Отже, для забезпечення ефективної кібербезпеки підприємства повинні системно здійснюватися: оцінювання ризиків, розроблення політик і процедур безпеки, використання сучасних технологій для захисту інформаційних систем, навчання персоналу та створення плану управління кіберінцидентами.

Список використаних джерел

1. Вавіленкова А. І. Методи і моделі протидії кібератакам : навчальний посібник. Київ : НА СБУ, 2023. 136 с.

2. Когут Ю. І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології) : практичний посібник. Київ : Консалтингова компанія «СІДКОН» ; ВД «Дакор», 2024. 284 с.

3. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році / Державна служба спеціального зв'язку та захисту інформації України. URL: https://scpc.gov.ua/uk/articles/334 (дата звернення: 14.11.2024).

4. Офіційна сторінка ситуаційного центру забезпечення кібербезпеки Служби безпеки України. URL: https://www.facebook.com/cybercentressu/ (дата звернення: 14.11.2024).

5. Про CERT-UA. URL: https://cert.gov.ua/about-us (дата звернення: 14.11.2024).

6. Загальні правила обміну інформацією про кіберінциденти. URL: https://cip.gov.ua/ua/news/zagalni-pravila-obminu-informaciyeyu-pro-kiberincidenti-protokol-tlp (дата звернення: 14.11.2024).

7. ENISA European Union Agency for CyberSecurity. URL: https://www.enisa.europa.eu/ (дата звернення: 15.11.2024).

8. Перелік категорій кіберінцидентів. URL: https://cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv (дата звернення: 15.11.2024).

9. Про основні засади забезпечення кібербезпеки України : Закон України, зі змінами та доповненнями. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 15.11.2024).

10. Посібник з додаткових ресурсів CRR. Т. 5: Управління кіберінцидентами. Copyright / Університет Карнегі-Меллона, 2016. 54 с.

11. Б'юкенен Б. Хакери і держави. Кібервійни як нові реалії сучасної геополітики / пер. з англ. Юлія Каздобіна. Київ : Наш Формат, 2024. 352 с.

Стаття надійшла до редакції 17.12.2024

UDC 004.056 (045)

Vavilenkova A. I.

THE CYBERINCIDENT MANAGEMENT PROCESS AS A NECESSARY STAGE IN THE ORGANISATION OF ENTERPRISE CYBERSECURITY

The article explores the main steps of the cyberincident management process, analyses the features of their organisation, and defines the role of cyberincident management within the overall cybersecurity framework of enterprises. This allows for the proper identification of priorities when developing an incident response and management plan to reduce system recovery time.

Each stage of the cyberincident management process is detailed, focusing on deliberate or accidental events that pose a threat to the security of information systems or networks and can lead to a disruption of their normal operation.

The cyberincident management process, which is an integral part of the overall cybersecurity strategy for enterprises, is viewed as a system involving detection, analysis, response, and mitigation of the consequences of destructive events. The first stage of the cyberincident management process is event detection, where certain situations are identified that could disrupt the organisation's regular activities. The second stage involves sorting and analysing events, i.e., classifying potential cyberincident and determining their priority for resolution. The third stage is response and recovery, which includes responding to the incident, limiting its impact, and minimising the damage caused by its occurrence. The fourth stage is improvement, which focuses on restoring normal system operations after the cyberincident has been localised and neutralised. Thus, the cyberincident management process is an essential component of the organisation's cybersecurity framework.

The conclusion is drawn that to ensure effective cybersecurity, enterprises must systematically implement risk assessment, development of security policies and procedures, use of modern technologies to protect information systems, staff training, and the creation of a cyberincident management plan.

Key words: *event detection, cybersecurity, cyber incident, cyber threat, cyber incident response, cyber incident management.*