МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ігор ПАВЛИЧУК
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Ігор ПАВЛИЧУК
Ім'я, ПРІЗВИЩЕ

Керівник: Юрій ЯКИМЕНКО
Д.в.н., доцент Ім'я, ПРІЗВИЩЕ

Рецензент:

Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Павличуку Ігорю Анатолійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Організація розслідування інцидентів інформаційної безпеки”, керівник кваліфікаційної роботи ЯКИМЕНКО Юрій, к.в.н.,доцент.
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій "Про закріплення тем випускних кваліфікаційних робіт та призначення наукових керівників на 2023-2024 н.р. за студентами першого (бакалаврського) рівня вищої освіти". № 36 від 27.02.24

2. Строк подання кваліфікаційної роботи «20» травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби забезпечення інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1. Проаналізувати теоретичні аспекти розслідування інцидентів інформаційної безпеки.
   4.2. Дослідити підходи до організації розслідування інцидентів інформаційної безпеки.
   4.3. Розробити рекомендації щодо покращення організації розслідування інцидентів інформаційної безпеки.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз теоретичних аспектів розслідування інцидентів інформаційної безпеки.	08.04.2024	
4.	Дослідження підходів до організації розслідування інцидентів інформаційної безпеки.	22.04.2024	
5.	Розробка рекомендацій щодо покращення організації розслідування інцидентів інформаційної безпеки.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Ігор ПАВЛИЧУК

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЯКИМЕНКО

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ на здобуття освітнього ступеня бакалавра

Направляється здобувач Павличук І.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Організація розслідування інцидентів інформаційної безпеки"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ПАВЛИЧУК Ігор у кваліфікаційній роботі проаналізував особливості управління інформаційною безпекою підприємства, дослідив основні засоби та методи захисту інформації на підприємств, вивчив засоби підвищення ефективності захисту інформації на підприємстві, розробив практичні рекомендації за темою дослідження.

ПАВЛИЧУК Ігор показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичній конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ПАВЛИЧУКА Ігоря на оцінку "добре" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЯКИМЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Павличук І.А. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ПАВЛИЧУКА Ігоря

на тему: «Організація розслідування інцидентів інформаційної безпеки»

Актуальність. Швидкий розвиток технологій, збільшення кількості підключених пристроїв та обсягів оброблюваних даних створюють серйозні виклики для забезпечення інформаційної безпеки. Однією з ключових причин актуальності цієї теми є постійне зростання кількості та складності кіберзагроз. Зловмисники прагнуть використовувати вразливості в системах безпеки для несанкціонованого доступу до конфіденційної інформації, крадіжки даних або впливу на нормальне функціонування організацій. Організація розслідування інцидентів інформаційної безпеки стає стратегічно важливою для забезпечення стабільності та надійності інформаційних систем. Клієнти, партнери та регулятори вимагають від компаній доказів того, що їхні системи належним чином захищені від можливих загроз. Важливо, щоб організації постійно контролювали та оцінювали свої методи розслідування інцидентів, щоб забезпечити їхню актуальність та ефективність у протидії новітнім загрозам. Значення вимірювання показників управління ризиками та оцінки ефективності заходів безпеки постійно зростає. Комплексний аналіз і оцінка ефективності розслідування інцидентів інформаційної безпеки є критичними аспектами для постійного вдосконалення систем управління ризиками та адаптації до змін у загрозах. Регулярне тестування і аудит процесів розслідування допомагають виявити слабкі місця та впровадити необхідні покращення для підвищення рівня інформаційної безпеки в організаціях.

Позитивні сторони. Кваліфікаційна робота охоплює важливу та актуальну тему, пов'язану з аналізом кіберзагроз в промислових системах та розробленням способів захисту, що відображає значущість цієї проблеми у сучасному цифровому світі. Кваліфікаційна робота вражає глибиною аналізу застосовуваних методик та підходів до аналізу кіберзагроз. Чітко структуровані

вступ та висновки роблять роботу добре організованою та логічно зв'язаною. Акцент на рекомендаціях щодо покращення організації розслідування інцидентів інформаційної безпеки є важливим аспектом роботи, що відображає сучасні тенденції у галузі інформаційної безпеки.

Недоліки. Хоча робота добре структурована, варто розглянути можливість більш детального аналізу окремих методик розслідування інцидентів інформаційної безпеки та їхнього порівняння, щоб надати читачеві глибше розуміння вибору конкретних підходів. Це дозволить визначити найбільш ефективні та відповідні методи реагування на кіберзагрози для різних типів організацій. Рекомендацією для майбутнього дослідження може бути розгляд можливості застосування обраних методик управління ризиками на конкретних прикладах чи в реальних умовах діяльності організацій. Такий підхід дозволить оцінити практичну ефективність методів та адаптувати їх до специфічних потреб і умов різних організацій, забезпечуючи максимальну ефективність реагування на кіберзагрози.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «добре», а здобувач ПАВЛИЧУК Ігор заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____

підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена оцінці ефективності засобів та методів захисту інформації на підприємстві. Робота складається зі вступу, трьох розділів, що містять 9 рисунків, 5 таблиць, висновків і списку використаних джерел із 45 найменувань, 2 додатки. Загальний обсяг роботи становить 67 аркушів, з яких 5 аркушів займають перелік умовних скорочень та список використаних джерел.

Об'єктом дослідження є інциденти інформаційної безпеки.

Предмет дослідження – особливості розслідування та реагування на інциденти інформаційної безпеки.

Метою роботи є організація розслідування інцидентів інформаційної безпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до організації реагування на інциденти інформаційної безпеки.

Як результат у роботі проаналізовано теоретичні аспекти розслідування інцидентів інформаційної безпеки, досліджено підходи до організації розслідування інцидентів інформаційної безпеки., розроблено рекомендації щодо покращення організації розслідування інцидентів інформаційної безпеки.

Галузь застосування. Розроблені підходи можуть бути використані при організації реагування на інциденти інформаційно безпеки.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ІНЦИДЕНТ, ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ, ПРОЦЕС УПРАВЛІННЯ ІНЦИДЕНТАМИ, ПІДХОДИ ДО ОРГАНІЗАЦІЇ РОЗСЛІДУВАННЯ, СТРАТЕГІЇ ПРОЦЕДУР РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ABSTRACT

The qualification work is dedicated to assessing the effectiveness of information protection tools and methods within an enterprise. The work consists of an introduction, three chapters containing 9 figures and 5 tables, conclusions, and a list of references with 45 entries, as well as 2 appendices. The total volume of the work is 67 pages, 5 of which are occupied by the list of abbreviations and the list of references.

The object the study is information security incidents.

The subject of the study is the peculiarities of investigating and responding to information security incidents.

The purpose of the study is to organize the investigation of information security incidents.

Research methods. In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, classification, expert assessment, systematic approach to organizing response to information security incidents.

As a result, the work analyzed the main theoretical aspects of investigating information security incidents, investagated approaches to organizing the investigation of information security incidents; developed recommendations for improving the organization of information security incident investigation.

Field of application. The developed approaches can be used in the organization of response to information security incidents.

Keywords: INFORMATION SECURITY, INCIDENT, ORGANIZATION OF INCIDENT INVESTIGATION, INCIDENT MANAGEMENT PROCESS, APPROACHES TO THE ORGANIZATION OF INVESTIGATION, STRATEGIES OF INCIDENT INVESTIGATION PROCEDURES, INFORMATION SECURITY MANAGEMENT.

ЗМІСТ

ВСТУП

Актуальність теми. У світі, де кіберзагрози стають все більшим викликом для організацій, забезпечення ефективної організації розслідування та реагування на ці загрози є важливим, як ніколи. Аналіз та оцінка ефективності засобів і методів реагування дозволяють визначити вразливості в системах безпеки та прийняти необхідні заходи для запобігання негативним наслідкам.

З огляду на зазначене, дослідження оцінки ефективності організації розслідування та реагування на інциденти інформаційної безпеки є актуальним науковим завданням.

Мета і завдання дослідження. ***Мета роботи*** полягає у організації розслідування інцидентів інформаційної безпеки.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати теоретичні аспекти розслідування інцидентів інформаційної безпеки.
2. Дослідити підходи до організації розслідування інцидентів інформаційної безпеки.
3. Розробити рекомендації щодо покращення організації розслідування інцидентів інформаційної безпеки.

Об'єкт дослідження – інциденти інформаційної безпеки.

Предмет дослідження – особливості розслідування та реагування на інциденти інформаційної безпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до організації реагування на інциденти інформаційної безпеки.

Як результат у роботі проаналізовано теоретичні аспекти розслідування інцидентів інформаційної безпеки, досліджено підходи до організації розслідування інцидентів інформаційної безпеки., розроблено рекомендації щодо покращення організації розслідування інцидентів інформаційної безпеки.

Практичне значення одержаних результатів. Застосування напрацювань дозволить здійснити правильну оцінку забезпечення безпеки інформації на підприємстві. Результати дослідження можуть допомогти оптимізувати систему реагування на кіберзагрози, ґрунтуючись на оцінці наявних методів та рекомендаціях щодо їх покращення. Це дозволить підприємствам швидше і ефективніше виявляти, реагувати на та усувати інциденти, мінімізуючи потенційні збитки та підвищуючи загальний рівень інформаційної безпеки.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ АСПЕКТИ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека є надзвичайно важливим аспектом у сучасному світі, де цифрова реальність набуває такого ж значення, як і фізична. Зі швидким розвитком технологій і постійним збільшенням кількості цифрових загроз, дослідження теоретичних аспектів розслідування інцидентів у сфері інформаційної безпеки стає особливо важливим.

Опанування теоретичних основ та методів розслідування інцидентів, що стосуються інформаційної безпеки, є ключовим етапом у боротьбі з цифровими загрозами. Це дає змогу не лише реагувати на виникнення таких інцидентів, але й запобігати їх появі, здійснюючи аналіз вразливих точок та слабких місць в інформаційних системах.

Дана тематика надає можливість для глибокого аналізу та розв’язання проблем, пов'язаних з інформаційною безпекою. Вивчаючи теоретичні аспекти розслідування інцидентів та основоположні принципи й методи, фахівці мають змогу розробляти більш ефективні стратегії захисту інформації та адекватного реагування на інциденти.

1.1 Місце розслідування в процесах управління інцидентами інформаційної безпеки

Сучасний розвиток інформаційних технологій потребує особливої уваги до безпеки даних. Розслідування інцидентів інформаційної безпеки набуває ключового значення для забезпечення захищеності інформаційних систем та протидії потенційним загрозам. Цей процес не тільки дозволяє виявити і нейтралізувати інциденти, але й запобігає їх повторенню в майбутньому. З огляду на важливість цієї діяльності, необхідно ретельно дослідити її основні етапи та забезпечити відповідну підтримку на всіх рівнях організації.

Розслідування інцидентів інформаційної безпеки займає центральне місце в управлінні цими інцидентами, включаючи ідентифікацію, аналіз і реагування на загрози та порушення безпеки. Важливо зазначити, що розслідування охоплює не лише фізичне місце події, але й інформаційне та технічне середовище, де стався інцидент.

Для кращого розуміння процесу розслідування інцидентів інформаційної безпеки, на рис. 1.1 наведена схема, яка ілюструє основні етапи цього процесу.

Рис. 1.1. Основні етапи розслідування в процесах управління інцидентами інформаційної безпеки [7]

Важливість місця розслідування полягає у спостереженні та виявленні інциденту. Це місце може бути будь-якою частиною інформаційної інфраструктури: корпоративною мережею, сервером або робочою станцією.

Виявлення інцидентів у контексті управління інформаційною безпекою є критично важливим процесом, спрямованим на ідентифікацію можливих або фактичних загроз безпеці. Цей етап є невід'ємною частиною циклу управління інцидентами і вимагає впровадження систем та методів, орієнтованих на

виявлення несправностей або неправомірних дій, що порушують конфіденційність, цілісність чи доступність інформації [7].

Розслідування інцидентів інформаційної безпеки вимагає глибокого розуміння контексту, в якому ці інциденти відбуваються. Це дозволяє не тільки ефективно реагувати на загрози, але й попереджати їх, аналізуючи вразливості та слабкі місця в системі. Таким чином, цей підхід забезпечує комплексний захист інформаційних систем і сприяє розвитку більш ефективних методів захисту даних.

Методи виявлення інцидентів включають перевірку логів подій, використання систем виявлення вторгнень (IDS) та систем виявлення аномалій (ADS), моніторинг мережевого трафіку, аналіз поведінки користувачів, а також застосування різних аналітичних інструментів для виявлення відхилень від звичайного режиму роботи системи. Як на мене, ці методи є дуже важливими, оскільки вони допомагають оперативно виявляти можливі загрози і мінімізувати шкоду від них [1;2].

Ефективність процесу виявлення інцидентів визначається не тільки можливістю вчасно виявляти порушення, але й тим, наскільки добре можна використати зібрану інформацію для подальшого аналізу та реагування. На мій погляд, такий підхід значно покращує стратегії захисту і дозволяє швидше реагувати на потенційні загрози, забезпечуючи високий рівень захисту інформаційних ресурсів [9, с. 63-64]. Це особливо актуально в сучасному світі, де інформаційна безпека стає все більш важливою.

Розслідування інцидентів охоплює збір доказів, які можуть підтвердити або спростувати факт інциденту. Це розслідування також надає можливість аналізувати логи подій, перевіряти системи та мережі для виявлення слідів діяльності зловмисників. Я вважаю, що цей процес є надзвичайно важливим для встановлення обставин інциденту і визначення його причин.

Збір доказів у контексті управління інцидентами інформаційної безпеки передбачає систематичний і об'єктивний процес збору, аналізу та документування різних елементів, які підтверджують або спростовують факт

інциденту або порушення безпеки в інформаційній системі або мережі. Це дійсно важливий етап, який допомагає визначити обставини інциденту і розробити ефективні стратегії реагування.

Для збору доказів використовуються різні джерела інформації, такі як логи подій систем, системні журнали, дані моніторингу мережі, а також інформація, отримана від спеціалізованих систем виявлення вторгнень та інших джерел. Ці докази можуть включати дані про аномальну активність, спроби вторгнення, зміни в системних налаштуваннях або інші дії, що свідчать про порушення безпеки. На мою думку, це надзвичайно важливо, оскільки дозволяє повноцінно зрозуміти, що саме сталося і як цього уникнути в майбутньому.

Процес збору доказів здійснюється відповідно до встановлених процедур і стандартів, які забезпечують їх цілісність, вірогідність і придатність для подальшого аналізу. Крім того, важливо дотримуватися вимог щодо збереження цілісності даних і забезпечення їх захисту від несанкціонованого доступу [10, с. 28].

Я вважаю, що дотримання цих вимог є ключовим для забезпечення об'єктивності розслідування і розробки ефективних заходів реагування. Ефективний збір доказів сприяє об'єктивному розслідуванню інцидентів, допомагає встановити обставини та причини їх виникнення, а також сприяє розробці ефективних стратегій для відновлення та запобігання подібним інцидентам у майбутньому [9].

На мою думку, це є надзвичайно важливо, оскільки дозволяє не тільки реагувати на інциденти, але й запобігати їм в майбутньому, що значно підвищує загальний рівень безпеки інформаційних систем.

Важливо зрозуміти, які фактори призвели до інциденту, а також оцінити його наслідки. Місце проведення розслідування дозволяє аналізувати системи, програми та дані для встановлення точного механізму виникнення інциденту. Аналіз причин і наслідків у контексті управління інцидентами інформаційної безпеки є складним процесом, спрямованим на виявлення і встановлення зв'язків між факторами, що спричинили інцидент, та його наслідками для інформаційної

системи або організації. Цей аналіз включає глибоке розуміння технічних, організаційних та людських аспектів інциденту з метою розробки ефективних стратегій реагування та запобігання подібним ситуаціям у майбутньому.

На рис. 1.2 показано етапи, які включає процес аналізу причин і наслідків. Цей процес допомагає виявити фактори, які призвели до інциденту, встановити їх взаємозв'язки та оцінити вплив на інформаційну систему або мережу. Таким чином, можна розробити стратегії та заходи для виправлення причин інциденту та мінімізації його наслідків у майбутньому (див. рис. 1.2).

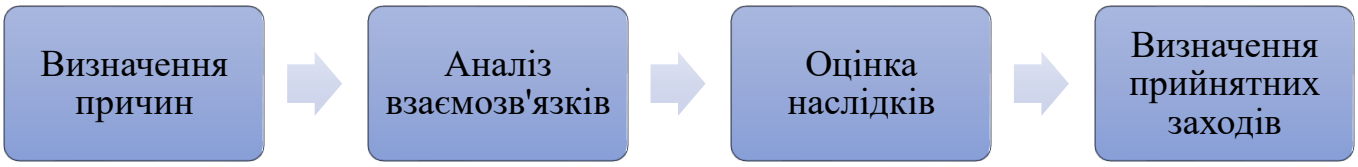

Рис. 1.2. Етапи, що входять до процесу аналізу причин і наслідків інциденту [13, с. 10-11]

Ідентифікація факторів, які призвели до виникнення інциденту, містить виявлення технічних вразливостей, недоліків у процесах управління безпекою, недбалість користувачів або зловмисні дії [13].

Наступним етапом є встановлення взаємозв'язків між різними причинами та оцінка їх впливу на інформаційну систему або мережу. Це дозволяє зрозуміти, як інцидент вплинув на організацію, включаючи можливі втрати даних, порушення конфіденційності, шкоду репутації та фінансові втрати.

Розробка стратегій та заходів для усунення причин інциденту і зменшення його наслідків у майбутньому є важливим етапом цього процесу. Ефективний аналіз причин і наслідків допомагає організаціям не тільки реагувати на інциденти, але й вдосконалювати свої процеси, технічні засоби та політики безпеки для запобігання подібним ситуаціям у майбутньому.

Після розслідування інциденту необхідно відновити роботу постраждалих систем та інфраструктури. Місце розслідування визначає стратегії відновлення,

включаючи виправлення вразливостей та відновлення даних. Відновлення роботи після інциденту інформаційної безпеки є критичним етапом у циклі управління інцидентами, що передбачає повернення до нормального функціонування інформаційних систем та процесів після виникнення порушень безпеки. На мою думку, цей процес має бути систематичним і організованим, з урахуванням всіх технічних, організаційних та процедурних аспектів [13, с. 3-4].

Підготовка до відновлення розпочинається ще на етапі передбачення, коли розробляються плани відновлення та резервування, визначаються ролі та відповідальність персоналу. Після виникнення інциденту основним завданням є оцінка обсягу робіт з відновлення, встановлення пріоритетів і порядок їх виконання.

Важливо забезпечити ефективну координацію між різними групами, залученими до відновлення роботи, щоб максимально використати наявні ресурси та уникнути дублювання зусиль. Технічні аспекти відновлення включають відновлення даних з резервних копій, відновлення налаштувань систем, а також відновлення фізичної або віртуальної інфраструктури [14, с. 17].

Водночас відновлення роботи після інциденту не обмежується лише технічними аспектами. Організаційні та комунікаційні елементи також відіграють ключову роль у забезпеченні успішного відновлення. Ефективна комунікація з зацікавленими сторонами, такими як керівництво, клієнти, партнери та громадськість, допомагає підтримувати довіру та знижувати негативні наслідки інциденту.

Отже, відновлення роботи після інциденту інформаційної безпеки є складним і багатоаспектним процесом, що потребує інтегрованого підходу, який охоплює технічні, організаційні та комунікаційні аспекти. На мою думку, здатність ефективно відновити роботу після інциденту визначається готовністю та компетентністю персоналу, наявністю належних процедур і планів відновлення, а також спроможністю вчасно реагувати на виниклі ситуації.

Результати розслідування надають можливість визначити ризики для подальшого запобігання подібним інцидентам. Місце проведення розслідування

стає базою для розробки та реалізації стратегій мінімізації ризиків у майбутньому.

Управління ризиками в контексті інформаційної безпеки є ключовим процесом, який включає ідентифікацію, аналіз, оцінку, контроль та зниження ризиків, що можуть виникнути внаслідок діяльності організації. Цей процес передбачає систематичний підхід до виявлення можливих загроз та вразливостей, а також розробку та впровадження стратегій для зниження впливу цих ризиків на організацію [13-14].

Перед тим як переходити до наступних кроків, важливо наголосити на важливості розслідування інцидентів для оцінки та управління ризиками. Розуміння того, які саме фактори спричинили інцидент, допомагає організації не тільки відновити нормальну роботу, але й запобігти подібним проблемам у майбутньому (див. рис. 1.3).

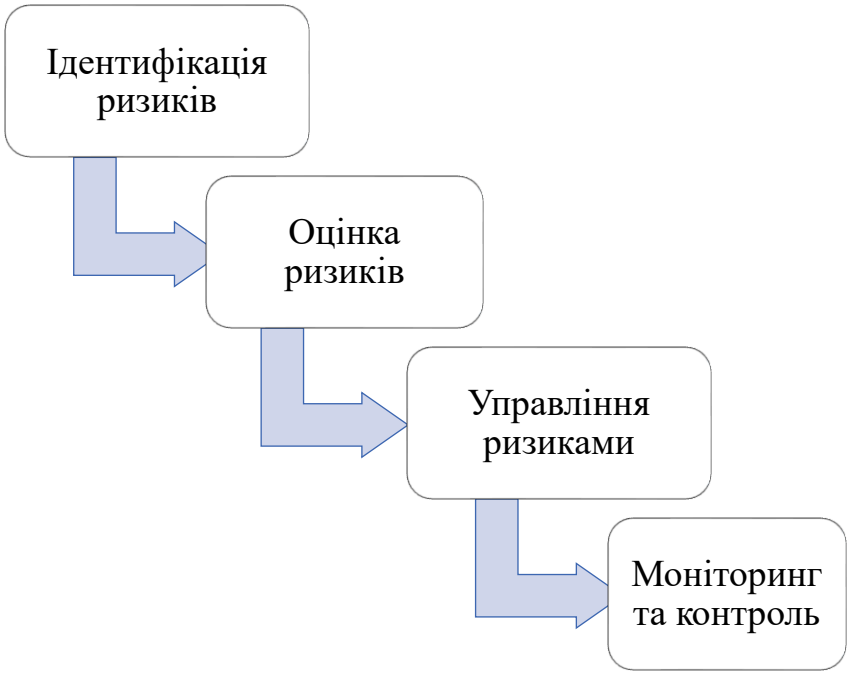

Рис. 1.3. Основні етапи управління ризиками [16]

Перший етап управління ризиками включає ідентифікацію потенційних загроз та вразливостей, які можуть вплинути на інформаційну безпеку організації. Ідентифікація ризиків охоплює аналіз як зовнішніх загроз, таких як

кібератаки чи природні катаклізми, так і внутрішніх, зокрема людські помилки або недоліки в організаційних процесах.

На етапі оцінки ризиків визначається ймовірність виникнення ризиків та їх потенційний вплив на організацію. Цей етап включає аналіз різних факторів, таких як ймовірність виникнення загроз, їхній вплив на інформаційні активи та можливі наслідки для бізнесу [16, с. 5].

Наступний етап управління ризиками передбачає розробку та реалізацію стратегій та заходів для зниження впливу виявлених ризиків на організацію. До таких заходів можуть належати розробка та впровадження захисних заходів, резервування даних, а також регулярний моніторинг та аудит системи безпеки.

Завершальний етап включає постійний моніторинг та контроль за рівнем ризиків та ефективністю заходів управління ризиками. У разі виявлення нових загроз або змін у наявних ризиках проводяться відповідні корекції стратегій управління ризиками.

Управління ризиками є невід'ємною частиною стратегічного планування та забезпечення безпеки інформації в організації. Ефективне управління ризиками допомагає зменшити ймовірність виникнення інцидентів та мінімізувати їхні наслідки для функціонування організації.

Місце розслідування інцидентів інформаційної безпеки відіграє важливу роль в процесі управління інцидентами, оскільки дозволяє організаціям ефективно виявляти, аналізувати та вирішувати інциденти, забезпечуючи безпеку та стабільність їх інформаційних ресурсів.

Місце розслідування функціонує як центральний вузол, де збирається, аналізується та обробляється інформація про інциденти в сфері інформаційної безпеки. Важливість цього процесу полягає у виявленні причин і наслідків інцидентів, розробці стратегій реагування та запобігання подібним ситуаціям у майбутньому, а також у відновленні нормального функціонування після інциденту.

Правильне проведення розслідування дозволяє організаціям не лише виявляти вразливі місця та порушення безпеки, але й вдосконалювати свої

системи та процеси для зменшення ризику та підвищення рівня захисту інформації. Такий підхід сприяє підвищенню відповідальності, ефективності та надійності управління інцидентами інформаційної безпеки.

Таким чином, місце розслідування є важливим компонентом управління інцидентами інформаційної безпеки, що допомагає організаціям стати більш стійкими та відповідати вимогам сучасного цифрового середовища.

1.2 Етапи розслідування інцидентів та методи його проведення

Розслідування інцидентів інформаційної безпеки включає кілька ключових етапів: підтвердження факту інциденту (чи не є він результатом природних чинників або катастроф); збір доказів по інциденту та визначення причин інциденту; об’єктів (відкрита інформація або з обмеженим доступом) та суб’єктів (співробітники, клієнти тощо), проти яких було спрямовано інцидент; місця та часу інциденту; засобів та методів здійснення атаки; розмірів збитків; винуватця або групи винуватців, а також осіб, які знали про наміри порушників і намагалися приховати сліди інциденту; мети порушення; причин, що сприяли успішній реалізації атаки; відповідних дисциплінарних заходів. Для успішного розслідування інциденту інформаційної безпеки важливими є швидкість і організованість дій групи реагування на інциденти.

Процес розслідування інцидентів інформаційної безпеки прийнято ділити на чотири етапи: збір; дослідження; аналіз; відображення [28]. Можна вважати, що до цього списку варто додати ще один етап – оцінювання області розслідування інцидентів інформаційної безпеки.

Перший етап – ініціювання розслідування, яке може бути спричинене різними джерелами:

- IDS (система виявлення вторгнень) фіксує переповнення буферу;
- повідомлення антивірусної програми;
- крах web-інтерфейсу;

– користувачі повідомляють про низьку швидкість при спробі виходу в Інтернет;

– системний адміністратор фіксує наявність файлів з підозрілими назвами;

– користувачі повідомляють про наявність у своїх поштових скриньках багатьох повторюваних повідомлень;

– хост вносить запис до журналу аудиту про зміну конфігурації;

– застосунок фіксує в журнальному файлі множинні невдалі спроби авторизації;

– адміністратор мережі фіксує різке збільшення мережевого трафіку [4, с. 112].

Правопорушення виявляються зазвичай:

– службами з питань інформаційної безпеки організацій внаслідок регулярних перевірок надійності системи доступу до інформації;

– випадково користувачами інформаційних систем;

– під час проведення бухгалтерських ревізій, аудиту;

– оперативним шляхом правоохоронними органами;

– у ході проведення дізнання та досудового слідства [2, с. 92].

Розслідування інцидентів у сфері інформаційної безпеки включає ряд ключових етапів, які сприяють ефективному управлінню загрозами та забезпеченню надійного захисту даних. Це дозволяє організаціям своєчасно реагувати на інциденти, виявляти їх причини та впроваджувати заходи для запобігання подібним ситуаціям у майбутньому.

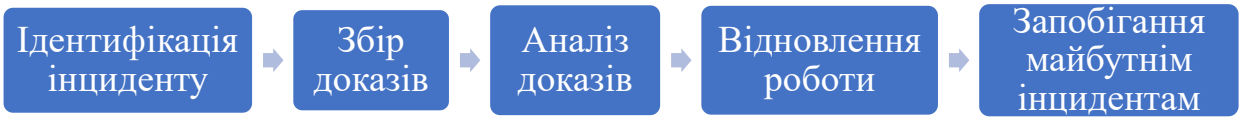

Рис. 1.4. Етапи розслідування інцидентів [18]

І. Перший етап розслідування полягає в ідентифікації інциденту або потенційної загрози для безпеки інформації. Це може бути здійснено шляхом постійного моніторингу систем, аналізу журналів подій, виявлення аномальних активностей або отримання повідомлень від користувачів [18]. Визначення інциденту є критичним для запобігання подальшому поширенню загрози та швидкої реакції на проблему.

Ідентифікація інциденту у сфері інформаційної безпеки включає систематичне виявлення та класифікацію подій або ситуацій, що можуть вплинути на захист інформації в організації. Це досягається за допомогою спеціалізованих технічних засобів моніторингу, аналізу журналів подій та виявлення аномальних активностей з метою раннього виявлення можливих загроз безпеці.

Процес ідентифікації включає моніторинг інформаційних потоків, аналіз системних журналів, мережевого трафіку, активності користувачів та інших інформаційних потоків. Це дозволяє виявити незвичайні або підозрілі активності, які можуть вказувати на потенційні загрози. Застосування алгоритмів машинного навчання та аналізу даних сприяє виявленню незвичайних паттернів або аномальних активностей, що можуть сигналізувати про можливі інциденти безпеки.

Після виявлення потенційних інцидентів вони класифікуються за типом, серйозністю та іншими характеристиками для подальшого аналізу та обробки.

Інформація про ідентифікований інцидент повідомляється відповідним сторонам, і приймаються заходи для реагування та подальшого розслідування. Ідентифікація інцидентів є першим і важливим етапом у процесі управління безпекою інформації, оскільки дозволяє організаціям реагувати на загрози найбільш ефективним чином та зменшувати час реакції на події безпеки [20, с. 6-7].

II. На етапі збору доказів здійснюється систематичне накопичення інформації про інцидент, включаючи журнали подій, системні журнали, дані моніторингу мережі, а також інформацію від спеціалізованих систем виявлення вторгнень.

Збір доказів у контексті управління інформаційною безпекою є процесом, що передбачає систематичний збір та аналіз різноманітної інформації, яка може бути використана для встановлення причин інцидентів, виявлення винних сторін, оцінки збитків та розробки стратегій запобігання подібним ситуаціям у майбутньому.

Процес збору доказів включає ідентифікацію джерел інформації, таких як журнали подій, системні журнали, дані моніторингу мережі та інші електронні джерела. Крок захоплення доказів включає збір фактичної інформації з зазначених джерел, яка може бути використана для подальшого аналізу. Це може включати копіювання журналів подій, витягів з баз даних, зберігання файлів та інші методи збору даних.

Зібрані докази необхідно належним чином зберігати та документувати для подальшого використання, включаючи можливе залучення до судових процедур або для забезпечення внутрішньої аудиторської відповідності. Збір доказів є критично важливою частиною процесу розслідування інцидентів, оскільки він надає об'єктивну та підтверджену інформацію, яка допомагає встановити факти, з'ясувати причини подій та прийняти відповідні заходи для запобігання подібним інцидентам у майбутньому [21, с. 147].

III. Після збору доказів вони піддаються детальному аналізу з метою визначення причин інциденту, виявлення вразливостей у системах або процесах та встановлення змін, які могли б запобігти подібним інцидентам у майбутньому.

Аналіз доказів у контексті розслідування інцидентів інформаційної безпеки є важливим етапом, що включає систематичне вивчення та інтерпретацію зібраних даних для встановлення обставин інциденту, визначення винних сторін та оцінки впливу на інформаційні системи. Цей процес базується на застосуванні методів цифрової криміналістики, аналітичних інструментів та експертних знань для формування повної картини події [21, с. 148-149].

Після збору доказів проводиться їх первинний огляд та систематизація, яка включає сортування даних, виділення ключових елементів та визначення пріоритетних напрямків аналізу. Первинний аналіз дозволяє структурувати дані та підготувати їх для подальшого детального розгляду. Одним із важливих методів аналізу є встановлення хронології подій, що дозволяє відтворити послідовність дій, які призвели до інциденту, та виявити ключові моменти, які можуть вказувати на причини та наслідки інциденту. Хронологічний аналіз допомагає виявити часові закономірності та кореляції між різними подіями.

Для більш глибокого розуміння інциденту важливо враховувати контекст, у якому сталися події. Це включає аналіз внутрішніх та зовнішніх факторів, які могли вплинути на інцидент, таких як мережеве середовище, політики безпеки, діяльність користувачів та інші умови [22, с. 14].

Інциденти, пов'язані з мережевою активністю, часто потребують аналізу мережевих журналів, трафіку та інших мережевих даних. Цей етап є важливим, оскільки він дозволяє виявити підозрілі з'єднання, передачу даних та інші аномальні дії, що можуть свідчити про загрозу безпеці.

Методи цифрової криміналістики використовуються для дослідження зібраних доказів. Це включає аналіз файлів, метаданих, системних журналів, знімків дисків та інших електронних даних. Форензичний аналіз допомагає виявити сліди злочинної діяльності, відновити видалені дані та забезпечити цілісність зібраних доказів.

Для більш глибокого розуміння інциденту важливо встановити взаємозв'язки між різними доказами. Кореляційний аналіз дозволяє виявити закономірності та зв'язки між подіями, що можуть вказувати на причини інциденту або надавати додаткову інформацію про його розвиток.

Результати аналізу повинні бути ретельно задокументовані та оформлені у вигляді звітів. Це включає детальний опис знайдених доказів, їх аналіз та висновки. Документація повинна бути зрозумілою та структурованою, щоб забезпечити її використання для подальших дій або юридичних процедур [21;22].

Аналіз доказів є складним і багатогранним процесом, що вимагає високої кваліфікації та використання спеціалізованих інструментів і методів. Метою є забезпечення об'єктивного та всебічного розуміння інциденту, що дозволяє приймати обґрунтовані рішення та вживати ефективні заходи для відновлення безпеки інформаційних систем і запобігання подібним інцидентам у майбутньому.

Після виявлення причин інциденту та прийняття відповідних заходів для їх виправлення проводиться відновлення роботи систем і процесів, які були порушені внаслідок інциденту.

IV. Після завершення аналізу та визначення причин інциденту наступним кроком є відновлення нормального функціонування систем. Це може включати відновлення даних з резервних копій, виправлення вразливостей, оновлення програмного забезпечення та налаштувань систем, а також проведення тестування для підтвердження відновлення роботи систем до нормального режиму. Важливо також враховувати навчання персоналу для підвищення їхньої обізнаності з питань інформаційної безпеки та запобігання повторенню подібних інцидентів у майбутньому [20;22].

Відновлення роботи після інциденту інформаційної безпеки є комплексним процесом, спрямованим на відновлення нормального функціонування інформаційних систем та забезпечення безперервності бізнес-процесів. Цей процес включає кілька етапів, які потребують координації між різними підрозділами організації, технічної компетентності та стратегічного

планування. Відновлення роботи є важливим аспектом управління інцидентами інформаційної безпеки, оскільки воно допомагає знизити вплив інцидентів на операційну діяльність і забезпечити стабільність бізнесу.

V. Завершальний етап процесу розслідування інцидентів полягає у розробці та впровадженні заходів для запобігання подібним інцидентам у майбутньому. Це може включати оновлення політик безпеки, впровадження нових технологій захисту, проведення навчань для співробітників та моніторинг нових загроз.

Запобігання майбутнім інцидентам передбачає аналіз виявлених вразливостей та ризиків, а також розробку стратегій та заходів для зменшення їхнього впливу на діяльність організації. Важливо також враховувати зміни у зовнішньому середовищі та нові загрози, які можуть виникнути у майбутньому.

Результати аналізу можуть використовуватися для оновлення політик та процедур безпеки, впровадження нових технологій захисту, проведення навчань для співробітників та підвищення їхньої обізнаності щодо потенційних загроз та заходів захисту. Ефективне управління ризиками допомагає зменшити ймовірність виникнення інцидентів та мінімізувати їхні наслідки для діяльності організації.

Після розслідування необхідно не лише виявити вразливості та порушення безпеки, а й вдосконалити свої системи та процеси для мінімізації ризику та підвищення рівня захисту інформації. Такий підхід сприяє підвищенню відповідальності, ефективності та надійності управління інцидентами інформаційної безпеки.

Після інциденту першочерговим завданням є оцінка масштабу та характеру завданих збитків. Це включає аналіз впливу інциденту на інформаційні системи, дані та бізнес-процеси. Важливо визначити, які компоненти системи були пошкоджені або знищені, які дані були втрачені або скомпрометовані, та які бізнес-процеси були порушені [23, с. 197].

На основі оцінки збитків розробляється детальний план відновлення. Цей план має включати визначення пріоритетів відновлення, ресурси, необхідні для відновлення, та розподіл ролей і відповідальності серед персоналу. План

відновлення також повинен враховувати можливі ризики та заходи для їх мінімізації.

Одним із ключових етапів є відновлення втрачених або пошкоджених даних. Це може включати відновлення з резервних копій, використання методів відновлення даних з пошкоджених носіїв або застосування інших технологій відновлення. Важливо забезпечити цілісність та конфіденційність відновлених даних.

Наступним кроком є відновлення роботи інформаційних систем, включаючи операційні системи, програмне забезпечення та апаратні засоби. Це може включати перевстановлення або оновлення програмного забезпечення, відновлення налаштувань системи, перевірку та тестування відновлених систем для забезпечення їх коректної роботи [31, с. 227].

Важливо також забезпечити відновлення порушених бізнес-процесів. Це включає координацію між різними підрозділами організації для забезпечення безперервності операцій, а також комунікацію з клієнтами та партнерами для інформування їх про стан відновлення та можливі затримки.

Після відновлення систем і процесів необхідно здійснити моніторинг та перевірку їх коректної роботи. Це включає проведення тестів на працездатність, перевірку на наявність залишкових вразливостей та оцінку ефективності відновлювальних заходів. Моніторинг дозволяє своєчасно виявляти та виправляти можливі проблеми.

Усі етапи відновлення повинні бути ретельно задокументовані. Це включає складання звітів про проведені дії, результати відновлення, виявлені проблеми та прийняті рішення. Документування є важливим для забезпечення прозорості процесу відновлення та його подальшого аналізу [31, с. 238-239].

На основі результатів відновлення проводиться аналіз процесів з метою їх поліпшення. Це включає внесення змін до планів безперервності бізнесу, вдосконалення політик і процедур безпеки, підвищення кваліфікації персоналу та впровадження нових технологій для підвищення рівня захисту.

Відновлення роботи після інциденту інформаційної безпеки є багатоступінчастим процесом, який вимагає ретельного планування, координації та використання сучасних технологій. Ефективне відновлення дозволяє мінімізувати вплив інциденту на діяльність організації та забезпечити стабільність і безперервність її операцій.

Останнім етапом є розробка і впровадження стратегій та заходів для запобігання подібним інцидентам у майбутньому. Це може включати оновлення політик безпеки, підвищення кваліфікації персоналу, впровадження нових технологій безпеки та регулярну перевірку систем безпеки [31;34].

Запобігання майбутнім інцидентам інформаційної безпеки є критично важливим аспектом управління безпекою, що включає розробку та впровадження стратегій, політик і процедур, спрямованих на мінімізацію ризику виникнення нових інцидентів. Цей процес базується на ретельному аналізі попередніх інцидентів, оцінці поточних вразливостей та прогнозуванні можливих загроз. Метою є створення стійкої та надійної системи безпеки, яка здатна ефективно протистояти різноманітним загрозам.

Детальний аналіз попередніх інцидентів є важливим кроком у розробці ефективних заходів запобігання. Це включає виявлення причин та умов, що сприяли виникненню інцидентів, аналіз слабких місць у системах безпеки та оцінку ефективності заходів, які були застосовані для реагування на інциденти. На основі цього аналізу розробляються рекомендації для покращення існуючих практик.

Регулярна оцінка ризиків дозволяє виявляти нові загрози та вразливості, які можуть вплинути на інформаційну безпеку організації. Це включає проведення аналізу ризиків, оцінку ймовірності та потенційного впливу загроз, а також визначення пріоритетів для впровадження заходів безпеки. Оцінка ризиків повинна проводитися на регулярній основі та оновлюватися у відповідь на зміни у внутрішньому та зовнішньому середовищі [34, с. 169].

Можна зазначити, що важливо не лише дотримуватися встановлених процедур і використовувати сучасні технології, але й постійно вдосконалювати

свої знання і навички в галузі інформаційної безпеки. Адже тільки постійне навчання та вдосконалення можуть забезпечити ефективний захист інформаційних ресурсів від нових і зростаючих загроз.

Розслідування інцидентів інформаційної безпеки є багатоступінчастим і складним процесом, що включає в себе виявлення інцидентів, збір і аналіз доказів, відновлення роботи систем та розробку заходів запобігання подібним інцидентам у майбутньому. Використання сучасних методів і технологій, таких як цифрова криміналістика та кореляційний аналіз, дозволяє забезпечити високий рівень захисту інформаційних систем та запобігати можливим загрозам.

На основі аналізу попередніх інцидентів і оцінки ризиків розробляються нові політики та процедури безпеки. Це можуть бути правила управління доступом, процедури резервного копіювання та відновлення даних, а також інструкції щодо використання мобільних пристроїв, спрямовані на підвищення захисту інформаційних ресурсів [39].

Використання сучасних технологій захисту є важливою складовою запобігання інцидентам. Це включає системи виявлення та запобігання вторгнень (IDS/IPS), брандмауери, антивірусне програмне забезпечення, шифрування даних та інші технології, які допомагають виявляти і блокувати загрози в реальному часі.

Людський фактор є одним із найуразливіших аспектів інформаційної безпеки. Тому необхідно проводити регулярні тренінги для персоналу, спрямовані на підвищення їхньої обізнаності про загрози та методи їх запобігання. Це включає навчання з безпечного використання інформаційних систем, розпізнавання фішингових атак, а також правил роботи з конфіденційними даними.

Постійний моніторинг інформаційних систем для виявлення потенційних загроз та аномальних активностей є надзвичайно важливим. Це включає використання систем SIEM (Security Information and Event Management), які дозволяють збирати, аналізувати та корелювати дані з різних джерел для

виявлення інцидентів. Своєчасне реагування на виявлені загрози дозволяє мінімізувати їхній вплив та запобігти їх подальшому розвитку [39, с. 77-78].

Розробка та впровадження планів реагування на інциденти і відновлення після них є критично важливими. Це включає створення інцидентних команд, визначення процедур реагування, проведення регулярних тренувань та тестування планів відновлення. Ефективне управління інцидентами дозволяє швидко відновити роботу систем та мінімізувати збитки.

Запобігання майбутнім інцидентам інформаційної безпеки є безперервним процесом, що потребує систематичного підходу та постійного вдосконалення. Використання передових практик, сучасних технологій і підвищення обізнаності персоналу дозволяє значно знизити ризик виникнення інцидентів і забезпечити стабільність та захищеність інформаційних ресурсів організації.

Методи проведення розслідування інцидентів можуть варіюватися в залежності від характеру інциденту і особливостей організації, але зазвичай включають використання технічних інструментів для збору і аналізу доказів, співпрацю з іншими відділами і експертами, а також застосування методів аналізу даних і розуміння характеру загроз. Важливо також забезпечити юридичну та етичну відповідність при проведенні розслідування.

Розслідування інцидентів не лише допомагає вирішити поточні проблеми, але і є стратегічним інструментом для виявлення вразливостей, аналізу причин інцидентів і запобігання подібним ситуаціям у майбутньому. Цей процес включає систематичний аналіз доказів, що дозволяє ідентифікувати причини інциденту і вжити відповідних заходів для відновлення роботи і запобігання майбутнім загрозам. Він також сприяє розробці стратегій управління ризиками і підвищенню готовності організації до майбутніх інцидентів [40].

Успішне розслідування інцидентів вимагає комплексного підходу, який включає технічні засоби, експертні знання і співпрацю між різними відділами та експертами. Важливо також дотримуватися відповідних юридичних та етичних стандартів під час проведення розслідування.

Отже, етапи розслідування інцидентів та методи їх проведення є важливими складовими управління безпекою інформації, які допомагають організаціям ефективно вирішувати поточні проблеми, а також підвищують рівень безпеки і готовності до майбутніх загроз.

Висновки до розділу 1

Отже, в розділі було розглянуто важливість та складність процесу розслідування інцидентів у контексті інформаційної безпеки. Вивчення цієї теми показує, що розслідування інцидентів є ключовим компонентом у забезпеченні захисту інформаційних систем і містить кілька основних етапів, які потребують детального розгляду.

Розслідування інцидентів в інформаційній безпеці є невід'ємною частиною процесу управління інцидентами. Цей процес дозволяє систематично виявляти, аналізувати та усувати загрози, що допомагає зменшити негативний вплив на організацію. Успішне розслідування не тільки вирішує поточні проблеми, але й попереджає майбутні інциденти через аналіз їх причин і впровадження запобіжних заходів.

Процес розслідування інцидентів інформаційної безпеки включає кілька основних етапів, серед яких:

1. Ідентифікація інциденту - швидке виявлення проблеми та ініціювання реагування.
2. Збір доказів - накопичення необхідної інформації для подальшого аналізу.
3. Аналіз причин і наслідків - визначення корінних причин інциденту і його наслідків.
4. Відновлення роботи - відновлення нормального функціонування систем і процесів.
5. Запобігання майбутнім інцидентам - розробка заходів для довготривалої безпеки.

Ці етапи є основою для забезпечення цілісності та точності розслідування. Загалом, розгляд теоретичних аспектів розслідування інцидентів інформаційної безпеки показує важливість системного та структурованого підходу до управління безпекою. Використання ефективних методів розслідування сприяє швидкому вирішенню інцидентів і створенню надійної системи безпеки, здатної протистояти новим загрозам.

Ключові фактори успіху включають використання сучасних технологій, постійне вдосконалення процедур безпеки та підвищення обізнаності персоналу. Ці заходи дозволяють організаціям мінімізувати ризики та забезпечити надійний захист своїх інформаційних ресурсів.

Розділ 2 АНАЛІЗ ПІДХОДІВ ДО ОРГАНІЗАЦІЇ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Порівняльний огляд основних методів розслідування інцидентів: реактивний та превентивний підходи

У сучасних умовах швидкого розвитку цифрових технологій та зростання кіберзагроз, організації стикаються з необхідністю обирати ефективні стратегії забезпечення інформаційної безпеки. Ключовими аспектами цих стратегій є вибір між реактивним і превентивним підходами до розслідування інцидентів. Реактивний підхід зосереджений на діях після інциденту, таких як виправлення вразливостей та мінімізація шкоди. Превентивний підхід, натомість, акцентує увагу на запобіганні загрозам через постійний моніторинг, регулярні оцінки безпеки та впровадження передових технологій. У цьому розділі проведено порівняльний аналіз основних методів розслідування інцидентів для визначення оптимальної стратегії забезпечення кібербезпеки організації.

Реактивний підхід до кібербезпеки фокусується на реагуванні на інциденти вже після їхнього виникнення. Основні кроки цього методу включають виявлення та виправлення відомих вразливостей, розслідування порушень і зменшення завданої шкоди. Попри необхідність таких дій для усунення загроз і відновлення системи, реактивна стратегія часто виявляється недостатньою при ізольованому застосуванні. Основний недолік цього підходу полягає в його нездатності передбачати та запобігати потенційним загрозам. Без проактивних заходів організації залишаються вразливими до повторних порушень і постійних ризиків [41, с. 856].

Зосередження виключно на реактивній стратегії кібербезпеки може мати кілька негативних наслідків. Наприклад, організація може стикнутися з повторними порушеннями безпеки через нездатність усунути корінні причини проблем. Це може призвести до значних операційних збоїв, підриваючи ефективність функціонування організації. Фінансові витрати на реактивний

підхід можуть бути значними, адже постійне реагування на інциденти потребує значних ресурсів, що може перенапружити бюджет організації та відволікти кошти від інших важливих сфер.

Реактивна стратегія часто призводить до фрагментарного підходу до безпеки, коли заходи впроваджуються від випадку до випадку. Відсутність комплексного плану безпеки створює прогалини у захисті, роблячи організацію вразливою до складних кіберзагроз. Крім того, час і зусилля, витрачені на реагування на інциденти, можуть перевантажити команду кібербезпеки, зменшуючи її здатність зосередитися на довгострокових стратегічних ініціативах [41;43].

Для зменшення ризиків та підвищення загального рівня кібербезпеки важливо впровадити збалансовану стратегію, яка включає проактивні елементи. Проактивний підхід передбачає передбачення потенційних загроз, проведення регулярних оцінок безпеки та впровадження передових заходів для запобігання інцидентам. Такий проактивний підхід не тільки зміцнює захист організації, але й забезпечує стабільне та безпечне операційне середовище. Поєднуючи реактивні та проактивні стратегії, організації можуть створити ефективну систему кібербезпеки, здатну протидіяти як поточним загрозам, так і довгостроковим ризикам [43].

Проактивний підхід до кібербезпеки полягає в тому, щоб передбачити та запобігти кіберзагрозам ще до того, як вони зможуть завдати шкоди. На відміну від реактивного підходу, який зосереджений на реагуванні на інциденти вже після їх виникнення, проактивна стратегія фокусується на постійному моніторингу та превентивних заходах. Це включає в себе безперервне спостереження за мережевою активністю, регулярну перевірку стану безпеки та впровадження сучасних методів захисту, які дозволяють своєчасно виявляти та усувати потенційні вразливості й загрози. Таким чином, підтримуючи актуальні протоколи безпеки, організації можуть забезпечити надійний захист від нових загроз.

Одним із важливих елементів проактивної стратегії є полювання на загрози. Це означає, що команди з безпеки активно шукають ознаки потенційних загроз у мережі, замість того, щоб чекати на сповіщення від автоматизованих систем. Мисливці за загрозами використовують поєднання передових інструментів та людської інтуїції для виявлення аномалій або підозрілих шаблонів, що можуть свідчити про можливе порушення. Такий підхід дозволяє виявити приховані загрози, які можуть залишитися непоміченими автоматизованими системами [44].

Аналітика в реальному часі є ще одним ключовим компонентом проактивної кібербезпеки. Завдяки аналізу даних у режимі реального часу, організації можуть оперативно виявляти підозрілу активність і реагувати на неї. Ця здатність до швидкого реагування є вирішальною для мінімізації впливу можливих інцидентів. Сучасні аналітичні інструменти здатні швидко обробляти великі обсяги даних, виокремлюючи аномалії, що потребують додаткового розслідування [44, с. 132].

Використання передових технологій, таких як штучний інтелект (ШІ) та машинне навчання (МН), значно підвищує ефективність проактивних заходів. Алгоритми ШІ та МН здатні аналізувати мережевий трафік і виявляти потенційні загрози, що дозволяє організаціям бути на крок попереду кібератак. Такі технології можуть адаптуватися до нових загроз, удосконалюючись на основі аналізу попередніх інцидентів. Наприклад, моделі машинного навчання можна навчити розпізнавати ознаки фішинг-атак або проникнення шкідливого програмного забезпечення, що дозволяє швидше і точніше ідентифікувати загрози.

Проактивний підхід також включає регулярні тести на проникнення та оцінку вразливостей. Тестування на проникнення моделює кібератаки для перевірки ефективності заходів безпеки, а оцінка вразливостей дозволяє виявити й усунути слабкі місця до того, як вони будуть використані зловмисниками. Ці заходи мають вирішальне значення для підтримання надійної системи безпеки і забезпечення захисту від нових загроз.

Крім того, проактивна стратегія кібербезпеки сприяє розвитку культури безпеки в організації. Регулярні тренінги та програми підвищення обізнаності допомагають співробітникам бути в курсі новітніх загроз і практик безпеки. Людський фактор є критичним, оскільки багато кібератак спрямовані на використання помилок і вразливостей співробітників [12, с. 178].

Займаючи проактивну позицію, організації можуть значно зменшити ризик кібератак і мінімізувати потенційні збитки. Такий підхід забезпечує більш безпечне робоче середовище та посилює загальну систему безпеки. Крім того, він підвищує здатність організації швидко та ефективно реагувати на інциденти, підтримуючи безперервність бізнесу та захищаючи критично важливі активи. Проактивна кібербезпека полягає не лише в запобіганні атакам, а й у створенні стійкої та адаптивної системи, яка може еволюціонувати разом із мінливим ландшафтом загроз.

Реактивний підхід зосереджується на реагуванні на інциденти після їх виникнення, що часто призводить до значних витрат на відновлення та розслідування. Натомість проактивний підхід спрямований на передбачення та запобігання загрозам, що дозволяє знизити витрати та підвищити стійкість системи. У наступній табл. 2.1 наведено порівняння ключових характеристик цих двох підходів, що допоможе краще зрозуміти їх переваги та недоліки.

Таблиця 2.1

Порівняння реактивного та проактивного підходу [12;17]

Характеристика	**Реактивний підхід**	**Проактивний підхід**
Основна мета	Реагування на інциденти після їх виникнення	Передбачення та запобігання загрозам до їх виникнення
Основні дії	Патчинг відомих вразливостей, розслідування інцидентів, мінімізація шкоди після інциденту	Постійний моніторинг, регулярні оцінки безпеки, впровадження передових заходів безпеки
Тип моніторингу	Реагування на виявлені інциденти	Постійний моніторинг та аналіз в реальному часі
Використання технологій	Стандартні інструменти для розслідування	Передові технології, такі як штучний інтелект та машинне навчання
Аналіз загроз	Після інциденту	Передбачення та аналіз потенційних загроз
Виявлення загроз	Після виникнення	На основі реального часу та прогнозування

Кошти	Високі витрати на відновлення та розслідування	Інвестиції у передові технології, економія на запобіганні інцидентам
Навантаження на персонал	Високе навантаження під час розслідування інцидентів	Постійна робота з передбачення та запобігання загрозам
Безпекова культура	Залежить від реагування персоналу на інциденти	Акцент на навчанні та підвищенні обізнаності про безпеку
Оцінка ризиків	Після інциденту, ретроспективний аналіз	Регулярні оцінки та аналіз для запобігання ризикам
Стійкість системи	Відновлення після інцидентів	Підвищена стійкість завдяки постійному вдосконаленню

Порівняння реактивного та превентивного підходів до кібербезпеки показує суттєві відмінності в методах і ефективності. Реактивний підхід фокусується на вирішенні проблем після їх виникнення, що важливо для негайного реагування та відновлення системи. Однак, його недоліками є високі витрати на відновлення і ризик повторних інцидентів через відсутність превентивних заходів.

Превентивний підхід включає постійний моніторинг, використання передових технологій, таких як штучний інтелект та машинне навчання, а також регулярні оцінки безпеки. Він спрямований на виявлення і запобігання загрозам до того, як вони зможуть завдати шкоди, що дозволяє значно знизити ризики кібернападів і зменшити витрати на відновлення [17, с. 318-319]. Витрати на такі технології окупаються завдяки запобіганню інцидентам.

Таким чином, для досягнення високого рівня кібербезпеки оптимально поєднувати обидва підходи, що забезпечує швидке реагування на інциденти та їхню ефективну профілактику. Це створює стійку систему захисту, здатну протистояти сучасним викликам.

Загалом, порівняння реактивного і превентивного підходів демонструє їхні переваги та недоліки. Реактивний підхід важливий для оперативного реагування, але призводить до високих витрат і ризику повторних атак. Натомість, превентивний підхід, використовуючи сучасні технології та регулярний моніторинг, забезпечує надійний захист і знижує ризики кібернападів. Інтеграція обох підходів дозволяє ефективно реагувати на інциденти та знижувати

ймовірність їх виникнення, що забезпечує стійкість та безпеку інформаційних систем організації.

2.2 Нові технології та інструменти для ефективного розслідування інцидентів

Незважаючи на впровадження адміністративного та технічного контролю за зниженням ризиків кібербезпеки, компанії все ще стикаються з інцидентами кібербезпеки та витоками даних. Не кожен інцидент закінчується витоком даних. Організація, яка може стримати зловмисника на ранній стадії ланцюжка знищення, може запобігти втраті даних і зменшити вплив інциденту. Оскільки команди безпеки працюють над тим, щоб реагувати на щоденний шквал сповіщень, їм потрібні інструменти, які дозволяють проводити швидкі розслідування для ефективного та результативного реагування на інциденти [21].

За останні два роки щорічна кількість розслідувань інцидентів інформаційної безпеки, проведених командою реагування на інциденти (IR) у Центрі експертної безпеки Positive Technologies (PT ESC), стабільно зростає. Наприклад, у 2022 році кількість таких розслідувань збільшилася на 50%, а за перші дев'ять місяців 2023 року порівняно з усім попереднім роком кількість проєктів зросла на 76%. Причиною такого значного зростання може бути збільшення кількості кіберінцидентів через недавні геополітичні та економічні події [35].

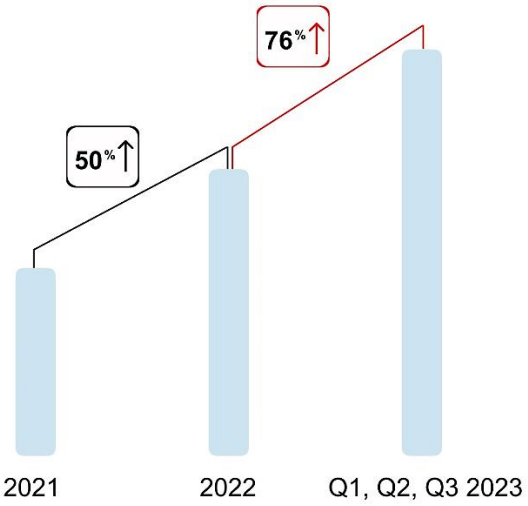

Рис. 2.1. Кількість проєктів з розслідування інцидентів у 2021-2022 рр та за 1—3 квартал 2023 року [35]

Для цього дослідження було проаналізовано інформацію з понад 100 проєктів, які можна класифікувати як розслідування інцидентів і ретроспективний аналіз інфраструктури. Ці проєкти проводилися з першого кварталу 2021 року по третій квартал 2023 року в різних компаніях. Більшість цих організацій (69%) представляють державні установи, промислові, фінансові та IT-компанії [35]. Більшість атак, які ми розслідували, були цілеспрямованими, тобто зловмисники мали на меті завдати шкоди конкретним компаніям.

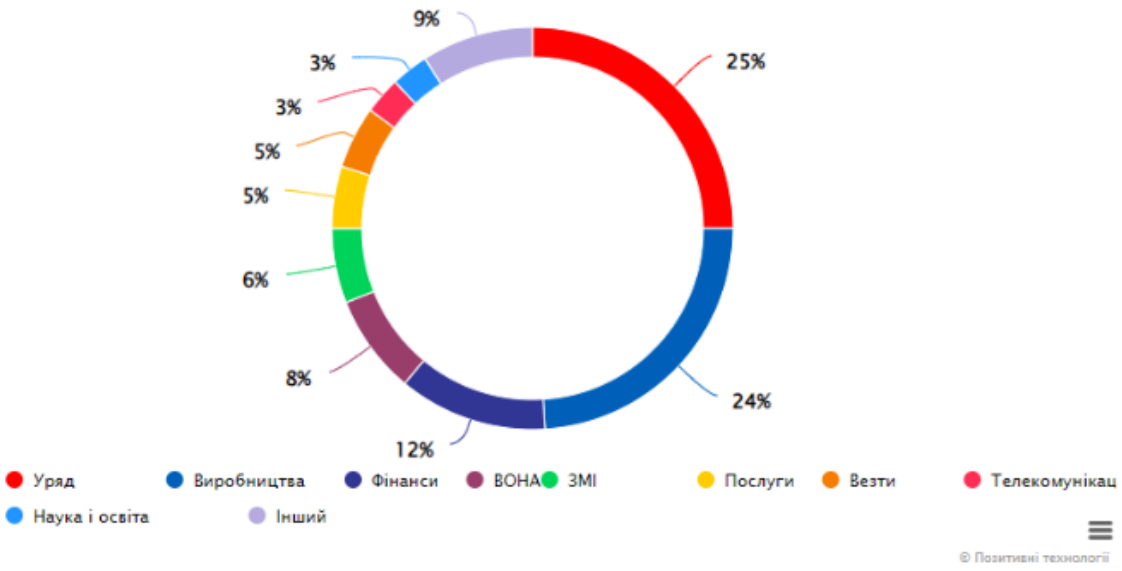

Рис. 2.2. Розподіл організацій-жертв за галузями [35]

Проаналізувавши проєкти з розслідування інцидентів та ретроспективні дослідження інфраструктури компаній, було встановлено, що 40% інцидентів були пов'язані з діяльністю відомих APT-груп, а решта 60% інцидентів стосувалися дій менш відомих груп або невизначених суб'єктів загрози, які діяли з метою фінансової вигоди або хактивізму, включаючи політичні цілі. Починаючи з 2022 року, було помічено зростання кількості політично вмотивованих інцидентів, які становили 9% від загальної кількості за досліджуваний період, що раніше не спостерігалося [35].

У швидкозмінному середовищі кібербезпеки здатність швидко та ефективно розслідувати інциденти має вирішальне значення. Організації повинні використовувати передові інструменти та методології, щоб випереджати загрози (див. рис. 2.3).

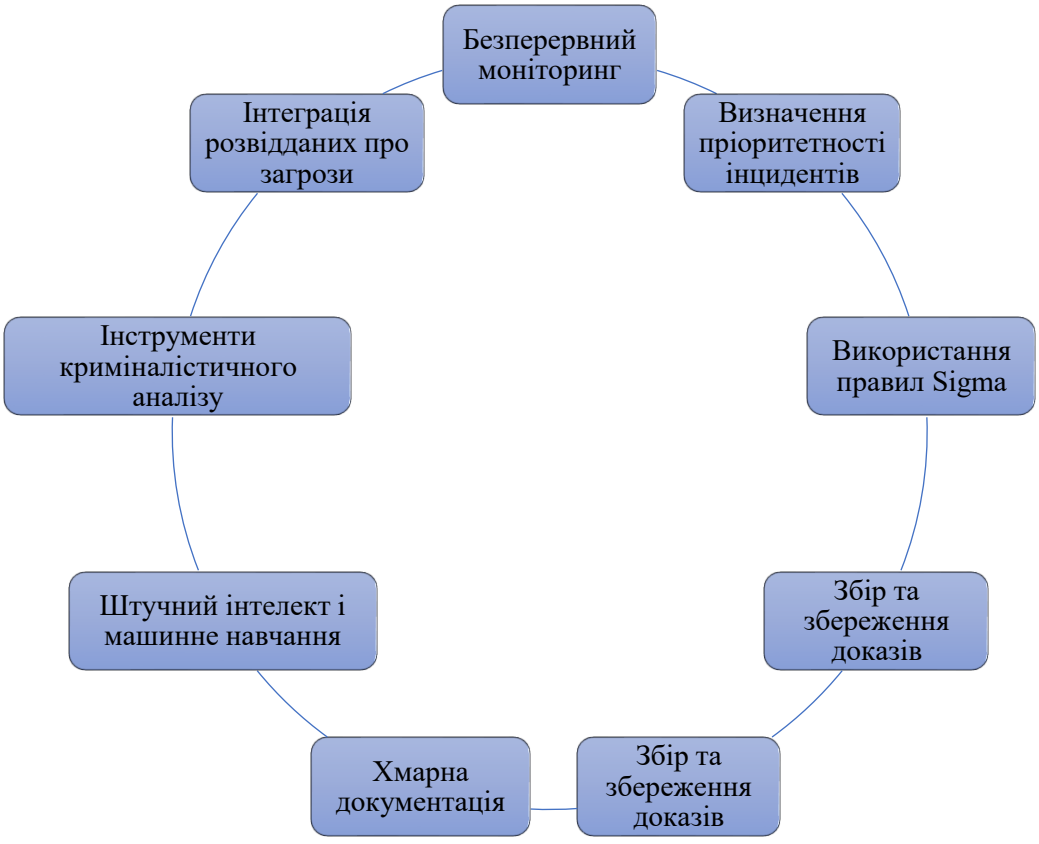

Рис. 2.3. Ключові стратегії для покращення розслідувань інцидентів кібербезпеки [24;25;26]

У сучасних умовах розслідування інцидентів кібербезпеки вимагають комплексного підходу та використання передових методів і технологій. Для забезпечення ефективного управління кіберзагрозами варто застосовувати низку ключових стратегій, які допоможуть покращити процеси виявлення, аналізу та реагування на інциденти. У дод. А представлено таблицю з основними стратегіями, які рекомендовані для покращення розслідувань інцидентів кібербезпеки.

Одна з основних стратегій – безперервний моніторинг. Він передбачає збір та аналіз даних з різних джерел для швидкого виявлення аномалій та загроз. Збираючи дані з мережевих пристроїв, серверів і додатків, організації можуть створити цілісну картину свого середовища і вчасно виявляти потенційні загрози.

Пріоритизація інцидентів допомагає розподіляти ресурси на найбільш критичні загрози. Щоденно в системах безпеки можуть з'являтися численні інциденти, і визначення пріоритетів на основі їхнього впливу дозволяє ефективніше використовувати час і зусилля команд безпеки [24, с. 62].

Правила Sigma – це стандартизовані формати для написання правил виявлення загроз, які можуть використовуватися на різних платформах. Це забезпечує узгодженість методологій виявлення та дозволяє швидко реагувати на відомі загрози.

Збір та зберігання доказів є важливим аспектом для забезпечення цілісності розслідування. Централізоване зберігання доказів дозволяє безпечно зберігати та аналізувати їх, що є ключовим для подальшого юридичного використання та розуміння характеру атаки.

Хмарна документація покращує координацію та ефективність команд. Використання хмарних рішень забезпечує віддалений доступ і можливість спільної роботи в реальному часі, що є критично важливим для команд, які працюють з різних місць [25, с. 1026-1027].

Штучний інтелект і машинне навчання допомагають автоматизувати процеси виявлення загроз і аналізу даних. Використання цих технологій

дозволяє виявляти закономірності та аномалії, які можуть бути пропущені при ручному аналізі.

Інструменти криміналістичного аналізу надають можливість глибокого аналізу векторів атак, що допомагає зрозуміти методи зловмисників та розробити ефективні стратегії захисту. Це включає такі методи, як аналіз пам'яті та криміналістика дисків.

Інтеграція розвідданих про загрози забезпечує цінну інформацію про нові загрози та профілі зловмисників, що допомагає командам безпеки краще зрозуміти загальний ландшафт загроз і ефективніше захищатися від них [26, с. 86].

Ці стратегії, детально описані в дод. А, є критичними для покращення розслідувань інцидентів кібербезпеки та забезпечення надійного захисту організацій.

Сучасні методи розслідування інцидентів кібербезпеки значно вдосконалюються завдяки використанню новітніх технологій та інструментів. Основні стратегії включають безперервний моніторинг, пріоритизацію інцидентів, застосування стандартних правил Sigma для виявлення загроз, а також централізоване збирання та зберігання доказів. Хмарні рішення для документації забезпечують масштабованість та підвищують ефективність співпраці. Інтеграція штучного інтелекту, машинного навчання, інструментів для форензики та автоматизації інцидентів допомагає значно покращити швидкість та якість розслідувань, забезпечуючи надійний захист від кіберзагроз.

2.3 Роль документування результатів розслідування інцидентів

Звітування про інциденти є критично важливим компонентом у підтримці безпеки на робочому місці та дотриманні нормативних стандартів. У цьому контексті незамінною є роль документації, яка слугує основою для фіксації та передачі точних деталей інцидентів, подальших розслідувань та впроваджених коригувальних заходів. Ретельне документування інцидентів гарантує, що кожен

аспект події буде зафіксований з точністю і ретельністю, забезпечуючи чіткий і всебічний звіт, на який можна посилатися і який можна аналізувати в майбутньому.

Документування результатів розслідування інцидентів є важливим елементом ефективного управління кібербезпекою. Дослідження показують, що в більшості випадків (96%), коли розслідування починалося, зловмисники все ще мали доступ до скомпрометованої інфраструктури або підтримували зв'язок з нею [35]. Медіанний час від моменту компрометації до виявлення (TTD) складав 37 днів, а в деяких випадках він міг досягати трьох років. Подробиці розподілу часу від компрометації до виявлення зловмисників представлені на рис. 2.4.

Ретельне документування кожного інциденту має вирішальне значення не тільки для аналізу поточних інцидентів, але й для створення бази даних для ретроспективного аналізу. Це дозволяє виявляти довготривалі атаки та потенційні вразливості в системі безпеки. Наприклад, середній час від початку розслідування до написання остаточного звіту складає 21 день, що підкреслює важливість своєчасного та детального документування всіх етапів розслідування.

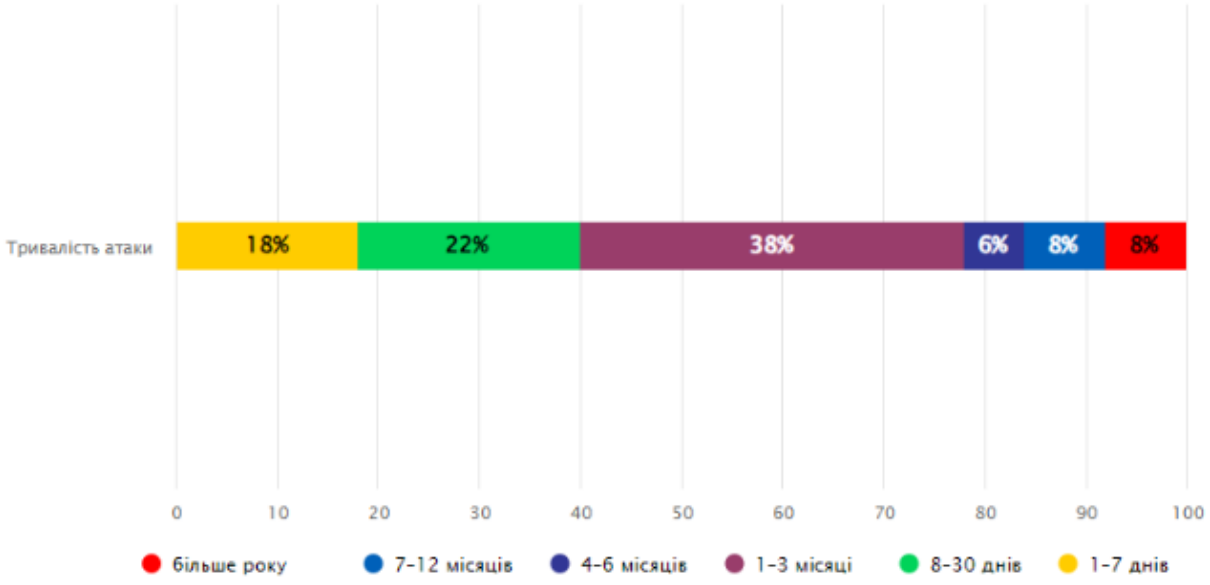

Рис. 2.4. Час від компрометації до виявлення зловмисників (Time to Detect, TTD) [35]

Завдяки детальному документуванню інцидентів, фахівці з інформаційної безпеки можуть не тільки оперативно реагувати на поточні загрози, але й розробляти заходи для запобігання майбутнім інцидентам. Це включає вдосконалення процесів моніторингу, впровадження нових технологій для виявлення загроз та розробку стратегій для швидкого реагування на кіберінциденти.

Протягом останнього часу найпоширенішими інцидентами були ті, що пов'язані з повним шифруванням або стиранням інформації на інфраструктурі замовника. Це становило 21% від загальної кількості інцидентів, розслідуваних протягом досліджуваного періоду [35]. У табл. 2.2 наведено список шкідливих програм, які використовуються для шифрування або стирання даних, виявлених під час розслідувань.

Таблиця 2.2

Список шкідливих програм для шифрування/стирання інформації, виявлених під час розслідувань інцидентів кібербезпеки [35]

№	Назва шкідливої програми	Опис
1	Омерта	Шифрує дані на комп'ютері та вимагає викуп за розшифровку.
2	Крихітка TinyCrypt	Легкий шифрувальник, який видаляє файли після шифрування.
3	Бабук та модифікації (BadWeather)	Вимагає викуп за доступ до зашифрованих даних.
4	Filecoder.MY	Шифрує файли та залишає повідомлення з вимогою викупу.
5	Засіб BitLocker	Використовує інструменти системного шифрування для блокування доступу до даних.
6	Фобос	Вимагає викуп за розблокування зашифрованих файлів.
7	Технологія CrossLock	Застосовує перехресне шифрування для утруднення розшифрування.
8	Шафка	Шифрує дані та залишає повідомлення з вимогою викупу.
9	Цепелін	Відома програма для шифрування даних з подальшим вимаганням викупу.
10	DiskCryptor	Використовує шифрування на рівні диска для блокування доступу до даних.
11	ЧорнийКокаїн	Агресивний шифрувальник, який повністю блокує систему.
12	CaddyWiper	Видаляє дані з диска, роблячи їх невідновними.
13	VoidCrypt	Шифрує дані та вимагає викуп за розшифровку.
14	Технологія LockBit	Використовує новітні методи шифрування для блокування доступу до даних.

15	РКРУ64	Використовує потужне шифрування для блокування доступу до файлів.

Документування результатів розслідування інцидентів кібербезпеки дозволяє не лише виявити і усунути поточні загрози, але й підготувати організацію до майбутніх викликів, використовуючи отримані дані для удосконалення стратегій захисту. Цей процес сприяє більш глибокому розумінню методів і тактик зловмисників, що дає можливість краще захистити організацію від можливих кіберзагроз у майбутньому.

Документування результатів розслідування інцидентів є надзвичайно важливим елементом кібербезпеки, що дозволяє детально фіксувати всі аспекти інциденту. Це включає точний запис дати, часу, місця, залучених осіб та послідовності подій. Така деталізація є критичною для розуміння природи інциденту, ідентифікації його першопричин та розробки плану подальших дій. Документація кожного аспекту інциденту перетворює звіт на цінний ресурс, який дозволяє слідчим відновити події, виявити сприятливі чинники та провести глибокий аналіз. Цей підхід не лише допомагає у вирішенні поточного інциденту, але й виявляє тенденції та повторювані проблеми, що дозволяє запровадити ефективні превентивні заходи для запобігання майбутнім загрозам [27;35].

Крім того, ретельне документування є необхідним для виконання законодавчих та нормативних вимог щодо звітування про інциденти. Багато законів зобов'язують організації вести точний облік всіх інцидентів, включаючи детальні звіти про розслідування та вжиті коригувальні заходи. Адекватне документування гарантує відповідність цим вимогам, що допомагає уникнути потенційних юридичних проблем і штрафів. Невиконання вимог щодо документування може призвести до значних юридичних та фінансових наслідків, які можуть негативно вплинути на репутацію та операційну ефективність організації [27].

Ретельне документування також сприяє підвищенню рівня підзвітності та прозорості в організації. Завдяки детальним записам про кожен інцидент, можна

чітко визначити, хто несе відповідальність за прийняті рішення і дії. Це сприяє формуванню культури довіри, відкритості та ефективної комунікації в організації, де всі учасники процесу розуміють свої обов'язки та відповідальність за результати.

Детально задокументовані звіти про інциденти та аналіз також покращують комунікацію і обмін знаннями між усіма зацікавленими сторонами. Організації можуть використовувати цю інформацію для розвитку культури навчання, де уроки, отримані з попередніх інцидентів, застосовуються для запобігання майбутнім. Така інформація стає цінним ресурсом для постійного вдосконалення процедур і впровадження найкращих практик, що в кінцевому результаті сприяє створенню безпечнішого та ефективнішого робочого середовища. За допомогою комплексного підходу до документування організації можуть підвищувати свою операційну стійкість і забезпечувати довгостроковий успіх.

2.4 Практичні приклади успішного впровадження підходів до розслідування інцидентів в сфері забезпечення інформаційної безпеки

Аналіз понад 100 проєктів розслідувань, проведених у різних компаніях, показав, що 40% інцидентів були пов'язані з діяльністю відомих APT-груп, а 60% - з менш відомими групами або іншими суб'єктами загроз. Успішне впровадження сучасних підходів до розслідування інцидентів, таких як інтеграція систем управління привілейованими обліковими записами та застосування принципу найменших привілеїв, дозволило значно зменшити час виявлення і реагування на інциденти. Ці практики допомогли мінімізувати негативні наслідки атак, включаючи втрату конфіденційної інформації та збої у бізнес-процесах [35]. Значна частина інцидентів (40%) протягом досліджуваного періоду була остаточно пов'язана з діяльністю відомих APT-груп. Розподіл жертв таких атак за галузями наведений на рис. 2.5.

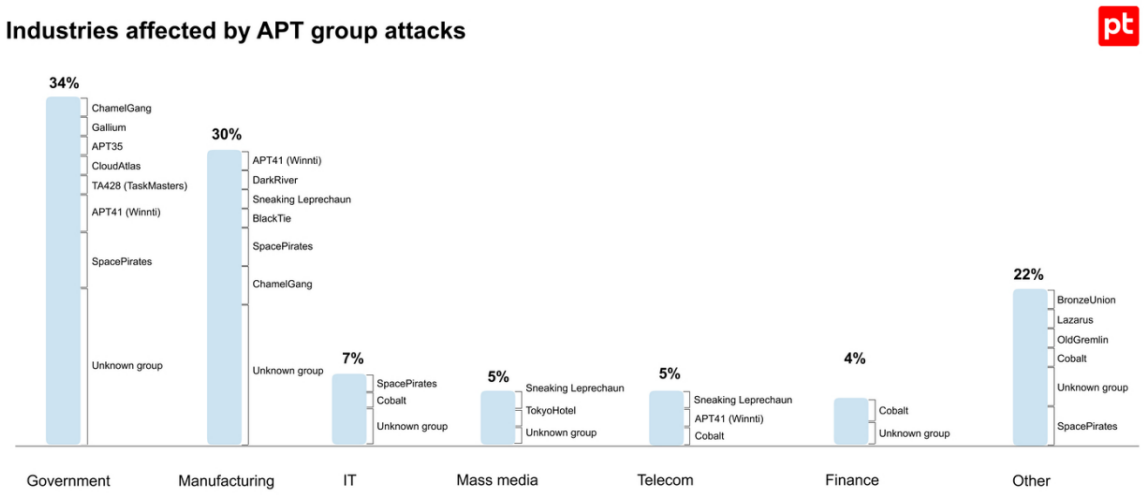

Рис. 2.5. Категорії жертв, які постраждали від групових атак APT [35]

APT-групи (Advanced Persistent Threat) зазвичай використовують унікальне шкідливе програмне забезпечення, яке надає їм доступ до корпоративних інфраструктур після початкової компрометації. В таблиці, яка наведена у дод. Б, можна знайти приклади такого програмного забезпечення. Ці програми забезпечують зловмисникам тривалий доступ до систем, що дозволяє їм збирати інформацію або здійснювати інші зловмисні дії.

Як APT-групи, так і менш кваліфіковані зловмисники часто використовують допоміжне програмне забезпечення, яке є у вільному доступі в інтернеті [35].

Атрибуція зловмисників – це складний процес, який не завжди дає надійні результати. Протягом останніх трьох років експерти з безпеки досліджували інциденти, пов'язані з 15 відомими APT-групами (Advanced Persistent Threats), які були ідентифіковані на основі використовуваних інструментів, мережевої інфраструктури та тактики, технік і процедур (TTP).

В рамках дослідження були розглянуті різні практичні приклади впровадження підходів до розслідування інцидентів, що дозволило визначити ключові фактори успішності та розробити рекомендації для підвищення ефективності розслідування та реагування на кіберінциденти (див. табл. 2.3).

Таблиця 2.3

Список виявлених груп APT [35]

№	Назва групи	Опис
1	APT35	Група, відома атаками на енергетичні сектори.
2	Хмарний атлас	Цілями атак є хмарні сервіси та корпоративні мережі.
3	Старий Гремлін	Атаки спрямовані на великі корпорації та урядові організації.
4	APT41 (Winnti)	Відомі атаки на компанії у сферах технологій та охорони здоров'я.
5	Кобальт	Здійснюють фінансові атаки на банки та фінансові установи.
6	Крадькома лепрекон	Цільові атаки на підприємства різних секторів.
7	BlackTie (TwistedPanda)	Здійснює атаки на урядові організації та великі компанії.
8	Темна річка	Направляє атаки на критичні інфраструктури.
9	Космічні пірати	Відомі атаками на телекомунікаційні компанії.
10	Бронзовий союз	Направляє свої атаки на військові установи та організації.
11	Галій	Група, що атакує енергетичний сектор та виробничі підприємства.
12	TA428 (TaskMasters)	Цільові атаки на урядові організації та великі корпорації.
13	ChamelGang (Банда ChamelGang)	Відомі атаками на фінансові та технологічні компанії.
14	Лазар	Спеціалізуються на атаках на великі підприємства та державні установи.
15	Готель Токіо	Здійснює атаки на урядові та комерційні структури.

Для глибшого розуміння практичних аспектів реагування на інциденти та управління ними у сфері інформаційної безпеки, варто звернути увагу на різноманітні тематичні дослідження та керівні принципи. Наприклад, комплексний процес управління інцидентами, запропонований Digital Guardian, підкреслює важливість багатостороннього підходу, який включає виявлення, повідомлення, оцінку та реагування на інциденти безпеки.

Один з важливих аспектів такого підходу – це створення чітко визначеної команди реагування на інциденти, де кожен член має свої конкретні ролі та обов'язки. Це забезпечує ефективність та результативність у процесі управління інцидентами. Крім того, документування та аналіз інцидентів виявляються ключовими елементами цього процесу, оскільки вони надають важливі дані для розуміння масштабу інциденту, вжитих заходів та отриманих уроків. Ці дані використовуються для вдосконалення майбутніх стратегій безпеки.

Наприклад, у випадку однієї великої компанії, чітко структурована команда реагування на інциденти дозволила швидко локалізувати та

нейтралізувати загрозу, завдяки чому було мінімізовано шкоду для бізнесу. Документування кожного кроку та детальний аналіз дій команди після інциденту дозволили виявити недоліки в існуючих процесах і внести необхідні зміни, що значно підвищило ефективність реагування на майбутні інциденти.

Для детального вивчення практичних аспектів реагування на інциденти кібербезпеки важливо аналізувати численні тематичні дослідження та рекомендації. Компанія Digital Guardian наголошує на важливості комплексного підходу до управління інцидентами, який охоплює етапи виявлення, звітування, оцінки та реагування на інциденти [29, с. 109-110]. Такий підхід підкреслює необхідність створення чітко структурованої команди реагування на інциденти, де кожен член має чітко визначені ролі та обов'язки, що забезпечує ефективність і результативність дій. Документування та аналіз інцидентів надає важливі дані для розуміння масштабу інциденту, вжитих заходів та досягнутих результатів. Це дозволяє організаціям визначати вразливі місця та розробляти стратегії для запобігання майбутнім інцидентам, підвищуючи загальний рівень безпеки.

Компанія CrowdStrike пропонує структурований підхід до реагування на інциденти, який включає підготовку, виявлення, аналіз, локалізацію, усунення та відновлення [30]. Такий підхід дозволяє організаціям оперативно та ефективно реагувати на інциденти, мінімізуючи шкоду і забезпечуючи безперервність бізнесу. Впровадження цієї системи сприяє створенню середовища, де кожен інцидент стає джерелом цінної інформації для вдосконалення майбутніх заходів реагування.

SentinelOne підкреслює важливість інтеграції розвідданих про загрози з автоматизованими системами розслідування інцидентів для підвищення швидкості та точності реагування. Їхній підхід передбачає постійне вдосконалення та адаптацію до нових загроз [29;30]. Завдяки цьому організації можуть швидко виявляти та реагувати на загрози, забезпечуючи ефективний захист своїх інформаційних активів.

Компанія StrongDM наголошує на важливості моніторингу в режимі реального часу, збору доказів та підтримки актуальних можливостей розвідки

загроз [32]. Це забезпечує негайне виявлення інцидентів та дозволяє швидко вживати заходів для їх усунення. Надійний збір доказів є критично важливим для розуміння впливу інциденту та підготовки до можливих юридичних або регуляторних дій.

Тематичне дослідження від HackerNoon надає приклад практичного застосування цих принципів, розглядаючи конкретний інцидент безпеки та детально описуючи кроки, вжиті на етапах розслідування і реагування [32]. Цей приклад показує, як теоретичні знання та рекомендації можна ефективно застосувати на практиці, забезпечуючи успішне управління інцидентами та підвищуючи рівень безпеки організації.

Синтезуючи знання з різних джерел, організації можуть розробляти та впроваджувати ефективні стратегії реагування на інциденти, які будуть комплексними, добре задокументованими та постійно вдосконалюватися для відповідності викликам сучасних кіберзагроз. Це забезпечує не тільки оперативне вирішення інцидентів, але й довгострокову стійкість та безпеку інформаційних систем організації.

Висновки до розділ 2

Аналіз понад 100 розслідувань інцидентів показав, що 40% інцидентів були пов'язані з діяльністю відомих APT-груп, а 60% – з іншими загрозами. Інтеграція сучасних підходів, таких як управління привілейованими обліковими записами і принцип найменших привілеїв, дозволила скоротити час на виявлення і реагування на інциденти, мінімізуючи негативні наслідки, такі як втрати даних та збої у бізнес-процесах.

Докладний аналіз виявив, що атаки були спрямовані на різні галузі, зокрема на енергетику, телекомунікації та фінансовий сектор. Зібрана інформація допомогла покращити заходи безпеки та підвищити готовність до майбутніх загроз.

Практичні підходи, як-от ретельне документування, створення спеціалізованих команд та інтеграція сучасних технологій, виявилися ефективними для підвищення рівня кібербезпеки. Це дозволяє організаціям швидко реагувати на інциденти і запобігати майбутнім загрозам, забезпечуючи довготривалу безпеку інформаційних систем.

Ефективне управління інцидентами включає як реактивні, так і превентивні заходи. Реактивні стратегії, як-от ті, що використовуються CrowdStrike, охоплюють усі етапи реагування від підготовки до відновлення, мінімізуючи збитки і постійно покращуючи стратегії. Превентивні заходи, такі як інтеграція аналітики загроз і автоматизованих розслідувань, які застосовує SentinelOne, забезпечують швидке виявлення і усунення загроз.

Практичне застосування цих підходів демонструє, як теоретичні принципи можна ефективно реалізувати, підвищуючи безпеку організації і знижуючи ризики.

Загалом, інтеграція сучасних підходів до розслідування інцидентів забезпечує ефективне управління загрозами, підвищуючи стійкість та безпеку інформаційних активів організацій.

Розділ 3 РЕКОМЕНДАЦІЇ ЩОДО ПОКРАЩЕННЯ ОРГАНІЗАЦІЇ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Розгляд стратегій покращення процедур розслідування інцидентів

У сучасному динамічному середовищі кібербезпеки організаціям потрібно адаптувати новітні технології, такі як машинне навчання (ML) та штучний інтелект (AI), щоб ефективно захищати свої цифрові активи. Традиційні методи безпеки вже не забезпечують достатнього захисту перед складними та швидко змінними кіберзагрозами. Інтеграція ML та AI у стратегії кібербезпеки значно покращує виявлення загроз, автоматизує аналіз інцидентів та підвищує точність моніторингу поведінки. Використання алгоритмів ML дозволяє виявляти аномалії, що можуть вказувати на потенційні загрози, забезпечуючи проактивний підхід до їх нейтралізації. Інструменти на основі AI допомагають швидко обробляти великі обсяги даних, виявляючи та пріоритизуючи інциденти за рівнем їхньої загрози, що дає змогу аналітикам більше зосередитися на складних задачах [33, с. 74-75].

Штучний інтелект може також створювати детальні моделі поведінки, що дозволяє точніше визначати аномальні дії, які можуть вказувати на складні загрози. Інтеграція AI та ML значно скорочує час виявлення та реагування на загрози, підвищуючи загальну ефективність кібербезпеки організації. Впровадження цих технологій стає необхідністю для організацій, які прагнуть забезпечити безпеку своїх критичних інформаційних систем в умовах постійно змінного ландшафту загроз.

Проактивний підхід до інформаційної безпеки, зокрема полювання на загрози, є критично важливим для виявлення та реагування на потенційні загрози. Полювання на загрози передбачає активний пошук загроз у системах організації, а не очікування на сповіщення. Це вимагає постійного моніторингу систем для виявлення будь-яких ознак компрометації або незвичної поведінки, що може свідчити про загрозу безпеці [37].

Для ефективного полювання на загрози організаціям потрібно створити надійну інфраструктуру моніторингу, яка б надавала інформацію про діяльність системи в реальному часі. Ця інфраструктура має використовувати передові аналітичні інструменти та технології, такі як машинне навчання, для виявлення аномалій. Постійний аналіз системних журналів, мережевого трафіку та інших даних дозволяє командам безпеки отримувати повне уявлення про загрози та швидко реагувати на нові ризики [37, с. 1222-1223].

Регулярне навчання команд реагування на інциденти є ще одним важливим аспектом проактивного підходу до безпеки. Часті тренінги забезпечують постійне оновлення знань членів команди щодо нових загроз та вразливостей, що підвищує їхню готовність до швидкого та ефективного реагування на інциденти. Навчальні програми повинні включати виявлення нових векторів атак, використання сучасних криміналістичних інструментів та впровадження кращих практик для стримування загроз.

Впровадження передових інструментів кібербезпеки, таких як системи управління інформацією та подіями безпеки (SIEM), є важливим для покращення ефективності та результативності заходів безпеки. SIEM-системи збирають, аналізують та корелюють дані з різних джерел у режимі реального часу, надаючи повну картину стану безпеки організації. Це дозволяє швидко виявляти потенційні загрози та реагувати на них до того, як вони завдадуть значної шкоди [36, с. 145].

Автоматизовані інструменти реагування на інциденти також відіграють ключову роль у сучасних системах безпеки. Вони допомагають виконувати рутинні завдання, такі як аналіз журналів і сортування сповіщень, що дозволяє командам безпеки зосередитися на більш складних проблемах. Автоматизація підвищує ефективність процесів реагування та знижує ймовірність людських помилок.

Рішення для виявлення та реагування на кінцевих точках (EDR) є важливими для забезпечення видимості дій усіх пристроїв у мережі. EDR-

інструменти дозволяють виявляти, розслідувати та реагувати на загрози на рівні кінцевих точок, забезпечуючи можливість відстежувати та аналізувати поведінку всіх пристроїв. Це підвищує здатність організацій виявляти та нейтралізувати складні атаки на кінцеві точки.

Створення комплексних політик і процедур є основою надійної системи кібербезпеки. Розробка та регулярне оновлення плану реагування на інциденти забезпечує чіткий та структурований підхід до управління загрозами. План повинен охоплювати всі етапи реагування від виявлення до відновлення і включати вказівки щодо координації між членами команди та іншими зацікавленими сторонами. Регулярне оновлення плану дозволяє враховувати нові загрози та зміни у структурі організації [1;41].

Чіткий розподіл ролей і обов'язків у команді реагування на інциденти забезпечує ефективне реагування на загрози. Кожен член команди має мати чітко визначену роль, що допомагає уникнути плутанини та забезпечує скоординовану реакцію. Це дозволяє організації швидко та ефективно реагувати на інциденти.

Аналіз після інциденту є важливим для постійного вдосконалення процесів реагування. Ретельний аналіз кожного інциденту дозволяє виявити отримані уроки та сфери для вдосконалення, що допомагає організаціям покращувати свої стратегії реагування та підвищувати готовність до майбутніх загроз [19].

Посилення збору та аналізу даних є ключовим для покращення захисту організацій від кіберзагроз. Одним з важливих кроків є централізація ведення журналів. Збираючи дані з різних джерел, таких як мережеві пристрої, сервери, додатки та кінцеві точки, організації можуть забезпечити повний доступ до всіх необхідних даних для всебічного аналізу. Це дозволяє створити цілісну картину стану безпеки і дає змогу швидше виявляти та реагувати на загрози. Центральне ведення журналів спрощує процес розслідування інцидентів і підвищує загальну ефективність управління кібербезпекою [33;45].

Інтеграція розвідданих про загрози також є важливою для покращення збору та аналізу даних. Інформація про нові загрози та методи атак (ТТП) допомагає організаціям бути в курсі останніх тенденцій у кіберпросторі та

готуватися до потенційних атак. Це дозволяє швидше і точніше виявляти загрози, реагувати на них до того, як вони завдадуть шкоди, і приймати обґрунтовані рішення щодо захисту [37].

Поведінковий аналіз є потужним інструментом для виявлення аномалій, які можуть свідчити про загрози. Аналізуючи відхилення від нормальної поведінки, організації можуть виявляти незвичну активність, що може вказувати на загрозу безпеці. Цей підхід дозволяє виявляти складні загрози, які можуть залишитися непоміченими при використанні традиційних методів. Поведінковий аналіз підвищує здатність організацій до виявлення та нейтралізації сучасних загроз [5, с. 29-30].

Посилення комунікації та співпраці є критичним для ефективної стратегії кібербезпеки. Внутрішня комунікація всередині команди та між відділами забезпечує своєчасний обмін інформацією і сприяє швидкому реагуванню на інциденти. Відкриті канали зв'язку дозволяють швидко передавати інформацію про потенційні загрози, що підвищує загальну готовність організації. Регулярні зустрічі та чіткі комунікаційні протоколи допомагають підтримувати високу обізнаність і готовність до дій.

Зовнішня співпраця з іншими організаціями, галузевими групами та державними установами є не менш важливою. Така співпраця дозволяє отримувати інформацію про нові загрози та ефективні методи захисту. Спільні зусилля сприяють кращому розумінню загроз і більш ефективному реагуванню на масштабні атаки. Участь у форумах та ініціативах з обміну інформацією допомагає організаціям залишатися в курсі останніх подій у сфері кібербезпеки.

Проведення регулярних навчань з моделювання інцидентів допомагає покращити комунікацію та співпрацю. Такі тренування дозволяють перевірити та вдосконалити процедури реагування на інциденти, виявляти слабкі місця і підвищувати готовність організації. Відпрацьовуючи різні сценарії, члени команди набувають досвіду, що дозволяє їм ефективніше діяти під час реальних інцидентів [11]. Ці навчання також дають можливість оцінити ефективність

каналів зв'язку та співпраці, що дає змогу впроваджувати вдосконалення та підвищувати загальну готовність.

Інвестиції у безперервне навчання та сертифікацію команди реагування на інциденти є критично важливими для підтримки високого рівня безпеки. Постійна освіта забезпечує, що члени команди володіють сучасними знаннями і навичками для ефективного виявлення та реагування на нові загрози. Це підвищує загальну компетентність і готовність команди до дій

Регулярний перегляд та оновлення інструментів безпеки дозволяє організаціям залишатися на крок попереду нових загроз. Періодичні оцінки ефективності інструментів допомагають виявляти слабкі місця і впроваджувати новітні рішення для покращення кіберзахисту. Модернізація інструментів дозволяє інтегрувати нові функції, що оптимізує роботу команди безпеки і підвищує її ефективність [6].

Використання ключових показників ефективності (KPI) допомагає вимірювати результативність процедур розслідування інцидентів. Аналізуючи ці показники, організації можуть виявляти недоліки і приймати рішення для вдосконалення своїх стратегій безпеки. Постійний моніторинг KPI сприяє розвитку культури підзвітності та постійному вдосконаленню [37].

Застосування машинного навчання та штучного інтелекту значно покращує здатність організації виявляти та аналізувати загрози. Машинне навчання дозволяє виявляти аномалії в поведінці систем, що сприяє проактивному виявленню загроз. Автоматизований аналіз на основі AI прискорює процес виявлення інцидентів та знижує навантаження на команди безпеки, забезпечуючи швидке реагування на загрози [38].

Поведінкове моделювання – це ще одна важлива сфера, де штучний інтелект може значно посилити заходи кібербезпеки. Використовуючи штучний інтелект для створення моделей типової поведінки в організації, системи безпеки можуть точніше виявляти аномалії, які можуть вказувати на загрозу. Ці моделі будуються шляхом аналізу історичних даних про звичайну поведінку користувачів, систем та додатків. Коли система помічає відхилення від цієї

норми, вона може сигналізувати про потенційну небезпеку для подальшого розслідування. Такий підхід особливо корисний для виявлення складних загроз, таких як інсайдерські атаки або APT-атаки, які часто не помічаються традиційними методами безпеки.

Інтеграція машинного навчання та штучного інтелекту в стратегії кібербезпеки є важливим кроком вперед у боротьбі з постійно зростаючими кіберзагрозами. Ці технології надають організаціям потужні інструменти для виявлення аномалій, що дозволяє проактивно виявляти потенційні загрози шляхом аналізу відхилень від встановлених норм. Автоматизований аналіз на основі штучного інтелекту допомагає швидко обробляти великі обсяги даних, забезпечуючи виявлення інцидентів і їх пріоритезацію, підвищуючи ефективність команд, які займаються реагуванням на інциденти.

Використання штучного інтелекту для створення детальних моделей поведінки дозволяє виявляти навіть найменші аномалії, що можуть вказувати на складні та тривалі загрози. Завдяки цьому організації можуть значно посилити свої системи безпеки, скоротити час на виявлення та реагування на загрози, а також підвищити загальну стійкість до динамічних кіберзагроз.

Отже, впровадження машинного навчання та штучного інтелекту є важливим для підтримання високого рівня кібербезпеки і захисту критично важливих цифрових активів у сучасному світі, який стає дедалі більш взаємопов'язаним. Ці технології допомагають організаціям ефективніше виявляти та запобігати загрозам, забезпечуючи надійний захист у швидкозмінному ландшафті кібербезпеки.

3.2 Нові технології та інструменти для ефективного розслідування інцидентів

Реагування на інциденти та їх розслідування є ключовими аспектами кібербезпеки, що дозволяють організаціям швидко виявляти загрози, усувати їх та мінімізувати негативні наслідки. Сучасні технології та інструменти значно

полегшують ці процеси, надаючи можливості для автоматизації, глибокого аналізу та інтеграції з іншими системами безпеки. Використання таких інструментів дозволяє не тільки ефективно реагувати на інциденти, але й здійснювати превентивні заходи, що запобігають повторним атакам.

На основі інформації з Hatica та Comparitech [8;15], нижче представлена табл. 3.1, що містить основні інструменти та технології, які використовуються для ефективного розслідування інцидентів.

Таблиця 3.1

Інструменти та технології для ефективного розслідування інцидентів [8;15]

Інструмент	Опис	Особливості
Splunk	Потужний інструмент для збору та аналізу даних з різних джерел у режимі реального часу.	Глибокий аналіз даних, моніторинг безперервних загроз, інтеграція з іншими системами.
Rapid7 InsightIDR	Інструмент для моніторингу та виявлення загроз, що забезпечує повний огляд діяльності в мережі.	Автоматичне виявлення аномалій, детальні звіти, підтримка гібридних середовищ.
SolarWinds Security Event Manager	Інструмент для моніторингу подій безпеки з можливістю аналізу та реагування на інциденти.	Автоматизація реагування, аналіз журналів, інтеграція з SIEM.
IBM QRadar	Система управління подіями та інформацією безпеки (SIEM) з можливістю аналізу та кореляції даних.	Машинне навчання для виявлення загроз, інтеграція з різними джерелами даних.
Cortex XDR	Інструмент для виявлення та реагування на загрози на кінцевих точках.	Комплексний аналіз загроз, інтеграція з іншими рішеннями безпеки.
Hatica	Інструмент для моніторингу та аналізу продуктивності команди, що працює з інцидентами.	Відстеження ефективності, збір даних про інциденти, підтримка роботи у віддаленому режимі.
Elastic Security	Інструмент для збору, аналізу та виявлення загроз у реальному часі з використанням відкритої платформи.	Безкоштовний доступ до даних, підтримка хмарних середовищ, аналіз у реальному часі.
Datadog	Інструмент для моніторингу та управління інцидентами у хмарних і гібридних середовищах.	Моніторинг у реальному часі, глибокий аналіз, інтеграція з DevOps.
AlienVault OSSIM	Відкрита система для управління безпекою та подіями з можливістю виявлення загроз та їх усунення.	Підтримка спільноти, інтеграція з іншими інструментами, гнучкість у налаштуваннях.
Snyk	Інструмент для безпеки програмного забезпечення з можливістю аналізу коду та виявлення вразливостей.	Аналіз вихідного коду, інтеграція з CI/CD, автоматичне виправлення вразливостей.

Сучасні інструменти для розслідування інцидентів дозволяють не тільки швидко реагувати на загрози, але й ефективно запобігати майбутнім атакам. Завдяки можливостям автоматизації та інтеграції з іншими системами, ці інструменти забезпечують високу ефективність та точність у виявленні та усуненні загроз [8].

Після впровадження таких інструментів, організація може значно знизити ризики, пов'язані з кіберзагрозами, та забезпечити надійний захист своїх інформаційних активів. Крім того, такі технології допомагають оптимізувати роботу команд безпеки, звільняючи їх від рутинних задач і дозволяючи зосередитися на стратегічно важливих питаннях кібербезпеки. Завдяки цьому, організація здатна швидко адаптуватися до нових викликів і забезпечити постійний захист своїх інформаційних систем [15].

Використання новітніх інструментів для розслідування інцидентів є невід'ємною частиною сучасної стратегії кібербезпеки, яка допомагає організаціям бути готовими до будь-яких загроз та підтримувати високий рівень безпеки у постійно змінному середовищі кіберпростору.

Реагування на інциденти та відновлення після них є ключовими елементами стратегії кібербезпеки будь-якої організації. Жодна компанія не може бути повністю захищена від зламів, тому важливо мати дієві механізми для швидкого відновлення даних і запобігання майбутнім атакам [37].

Відновлення після кібератак вимагає використання спеціалізованих інструментів і методів для швидкого відновлення критичної інформації. Це включає не тільки резервне копіювання даних, але й застосування сучасних технологій для відновлення пошкоджених файлів і систем, що мінімізує простої та втрату даних.

Аналіз інцидентів передбачає ретельне вивчення деталей для визначення причин та наслідків атаки. Це допомагає виявити слабкі місця та уникнути повторення подібних подій у майбутньому. Наприклад, аналіз журналів системи та мережевого трафіку може показати, як відбулася атака і хто за нею стоїть.

Після такого аналізу можуть бути внесені зміни в політики безпеки або впроваджені нові технології захисту, щоб запобігти майбутнім атакам. Це може включати оновлення програмного забезпечення, налаштування мережевих бар'єрів та додаткові заходи безпеки [37;43].

План відновлення після інциденту повинен містити стратегії для відновлення ключових функцій організації. Це включає резервне копіювання даних, відновлення фізичних приміщень, апаратного та програмного забезпечення, а також співпрацю з постачальниками та іншими зовнішніми партнерами. Ефективне реагування на інциденти вимагає ретельного планування, тренувань персоналу, регулярного тестування планів та постійного оновлення процедур у відповідь на зміни в технологіях і загрози кібербезпеки. Регулярне навчання та оновлення знань співробітників допомагає забезпечити готовність організації до будь-яких кіберінцидентів.

Компанія DigVel, наприклад, надає комплексні послуги з кібербезпеки, включаючи оцінку стану безпеки, впровадження заходів захисту, розслідування інцидентів та DevSecOps. Це дозволяє забезпечити повний захист інформаційних систем і даних організації, знизити ризики кібератак і мінімізувати їхні наслідки.

Отже, реагування на інциденти та аварійне відновлення є критичними компонентами кібербезпеки. Правильне планування, аналіз і впровадження заходів захисту можуть значно знизити ризики і забезпечити безперебійну роботу організації навіть у разі кіберінцидентів. Це дозволяє організаціям бути готовими до будь-яких викликів у сфері кібербезпеки.

3.3 Заходи щодо підвищення кваліфікації персоналу та підготовки до розслідування інцидентів

Підвищення обізнаності про кібербезпеку серед співробітників є важливим елементом захисту організацій від кіберзагроз. Для забезпечення ефективного навчання працівників необхідно регулярно проводити тренінги з кібербезпеки, щоб вони були в курсі новітніх загроз та методів захисту. Навчання

співробітників розпізнавати фішингові атаки є критично важливим, оскільки такі атаки часто використовуються зловмисниками для отримання доступу до систем організації. Це включає в себе пояснення того, як виглядають фішингові електронні листи, які ознаки можуть свідчити про спробу обману, і як правильно реагувати на підозрілі повідомлення. Практичні тренінги, де співробітники можуть імітувати реальні ситуації, також є ефективним методом підвищення їхньої обізнаності та навичок у сфері кібербезпеки.

Таблиця 3.2

Заходи щодо підвищення кваліфікації персоналу в кібербезпеці [1;3;6]

Захід	Опис
Регулярні тренінги	Проведення навчальних занять з виявлення загроз, особливо фішингових атак, для підвищення обізнаності співробітників.
Багатофакторна аутентифікація	Впровадження додаткових заходів безпеки, таких як SMS-коди або біометричні дані, для доступу до системи.
Використання надійних паролів	Навчання співробітників створювати складні паролі та використовувати менеджери паролів для зберігання та генерації унікальних паролів.
Своєчасне оновлення ПЗ	Встановлення оновлень і патчів для програмного забезпечення та операційних систем, щоб захистити від нових вразливостей.
Моніторинг і аудити	Постійне спостереження за системами та проведення регулярних аудитів безпеки для виявлення слабких місць і покращення заходів захисту.
Відкриті канали спілкування	Підтримка політики, що заохочує співробітників повідомляти про підозрілі активності без страху перед наслідками.
Впровадження сучасних технологій	Використання систем виявлення та запобігання вторгненням, а також регулярне тестування на проникнення.

Перед тим як розглянути табл. 3.2, важливо зазначити, що підвищення обізнаності про кібербезпеку серед співробітників є важливим аспектом захисту організацій від кіберзагроз. Це допомагає запобігти багатьом атакам, оскільки людський фактор часто є найслабшою ланкою в системі безпеки.

Після впровадження цих заходів, організація може значно знизити ризики, пов'язані з кіберзагрозами, та забезпечити надійний захист своїх інформаційних активів. Навчання співробітників та використання новітніх технологій значно підвищують ефективність безпеки організації. Важливо, щоб кожен працівник розумів свою роль у підтримці безпеки та активно брав участь у заходах, спрямованих на захист організації.

Отже, впровадження регулярних тренінгів, багатофакторної аутентифікації, використання надійних паролів, своєчасне оновлення ПЗ, постійний моніторинг та підтримка відкритих каналів спілкування є ключовими заходами, які сприяють підвищенню кваліфікації персоналу та готовності до розслідування інцидентів. Важливо також підтримувати культуру кібербезпеки, де кожен співробітник усвідомлює свою відповідальність за захист даних організації.

Ці дії допомагають організаціям не лише реагувати на існуючі загрози, але й проективно захищати себе від нових потенційних атак. У підсумку, комплексний підхід до підвищення обізнаності про кібербезпеку серед співробітників, впровадження передових технологій захисту та створення культури відповідальності є ключем до успішної кібербезпеки будь-якої організації. Це включає не лише технічні заходи, але й формування усвідомлення серед співробітників щодо важливості їхньої ролі в забезпеченні безпеки. Організація повинна постійно інвестувати в навчання, розвиток та мотивацію працівників для створення стійкого і надійного захисту від кіберзагроз.

3.4 Використання методики організації розслідування інцидентів при управлінні інформаційною безпекою - на прикладі

Управління інцидентами інформаційної безпеки в великих організаціях є складним процесом, який складається з кількох важливих етапів: виявлення, аналіз, реагування та відновлення. На прикладі показано, як впровадження методики розслідування інцидентів може суттєво покращити захист організації від кіберзагроз.

Перш ніж перейти до розгляду кожного етапу, важливо зрозуміти, що систематичний підхід до розслідування інцидентів дозволяє організаціям не тільки швидко реагувати на поточні загрози, але й запобігати їх повторенню у майбутньому. Кожен етап процесу має свої специфічні завдання, які

допомагають зменшити негативний вплив інцидентів на бізнес-процеси та забезпечити безперебійну роботу системи.

Основні етапи розслідування інцидентів:

I. Перший крок у розслідуванні інциденту – це виявлення підозрілої активності чи аномалій у системах організації. Це може включати моніторинг мережевих пристроїв, серверів та користувацької активності для виявлення можливих загроз. Важливо мати ефективні інструменти для моніторингу та аналізу, які здатні виявити навіть найменші відхилення від норми.

II. Наступний етап передбачає детальний аналіз інциденту для визначення його природи та причин. Фахівці з безпеки аналізують зібрані дані, щоб зрозуміти, як і чому відбувся інцидент, які вразливості були використані та які системи постраждали. Це допомагає розробити заходи для запобігання повторенню таких інцидентів.

III. Після аналізу інциденту необхідно вжити заходів для мінімізації його впливу. Це може включати блокування шкідливих дій, відновлення нормальної роботи систем і вжиття заходів для запобігання подібним інцидентам у майбутньому. Важливо також комунікувати з усіма зацікавленими сторонами, такими як керівництво організації, постраждалі користувачі та зовнішні організації, якщо це необхідно [1].

IV. Заключний етап передбачає відновлення систем до нормального стану та впровадження додаткових заходів для підвищення рівня безпеки. Це може включати оновлення програмного забезпечення, зміну політик безпеки та проведення навчань для персоналу. Важливо також провести аналіз проведених заходів для покращення процесів управління інцидентами та підготовки до майбутніх загроз.

Після розгляду основних етапів управління інцидентами, варто відзначити, що кожен з них є критично важливим для забезпечення надійного захисту організації. Ефективне управління інцидентами дозволяє зменшити час простою систем, знизити ризик втрати даних та мінімізувати фінансові збитки, пов'язані з кіберінцидентами.

Використання методик управління інцидентами не тільки забезпечує надійний захист інформаційних активів, але й сприяє підвищенню загального рівня безпеки в організації. Це включає інтеграцію з іншими процесами управління безпекою, такими як управління ризиками, аудит безпеки та відповідність нормативним вимогам, що дозволяє створити комплексний підхід до забезпечення кібербезпеки [42].

Важливо зазначити, що успіх у впровадженні методик розслідування інцидентів багато в чому залежить від кваліфікації персоналу та ефективності використання спеціалізованих інструментів і технологій. Злагоджена робота команди, чіткі процедури та постійне вдосконалення заходів безпеки є ключовими факторами для успішного управління інцидентами та забезпечення безпеки організаційних систем і даних [15;38].

Для досягнення високої ефективності в управлінні інцидентами важливо, щоб організація мала чітко визначені політики та процедури, які регулюють дії у разі виникнення інциденту. Це дозволяє не тільки швидко реагувати на загрози, але й забезпечує узгодженість дій усіх задіяних сторін. Крім того, постійне навчання та підвищення кваліфікації співробітників допомагає тримати їх в курсі нових загроз і методів захисту, що є ключовим для підтримання високого рівня кібербезпеки [1;11].

Висновок до розділу 3

Дослідження показало, що ефективне управління інцидентами інформаційної безпеки потребує використання сучасних технологій, таких як машинне навчання та штучний інтелект. Ці технології допомагають автоматично виявляти загрози, аналізувати їх і швидко реагувати на них, що значно підвищує безпеку організації.

Проактивний підхід до кібербезпеки, який включає постійний моніторинг і виявлення загроз, є ключовим для зниження ризиків. Важливо створити надійну

інфраструктуру моніторингу та регулярно навчати команду, щоб вони завжди були готові до нових викликів.

Використання систем управління інформацією та подіями безпеки (SIEM) дозволяє зібрати всі необхідні дані з різних джерел і швидко виявити потенційні загрози. Це допомагає оперативно реагувати на інциденти і забезпечувати безпеку даних.

Автоматизація процесів реагування на інциденти значно знижує навантаження на команди безпеки та підвищує ефективність їхньої роботи. Це дозволяє швидко реагувати на загрози і забезпечувати стабільну роботу організації.

Загалом, використання сучасних технологій і проактивного підходу до кібербезпеки допомагає організаціям ефективно управляти інцидентами, мінімізуючи ризики і забезпечуючи безперебійну роботу навіть у разі кіберінцидентів.

ВИСНОВКИ

Дослідження організації розслідування інцидентів інформаційної безпеки дозволило зробити кілька важливих висновків. Розслідування інцидентів інформаційної безпеки є невід'ємною частиною процесу управління інформаційною безпекою. Ефективне розслідування дозволяє не тільки усунути наслідки інциденту, але й запобігти майбутнім загрозам завдяки аналізу причин та розробці превентивних заходів. Виявлено, що процес розслідування складається з кількох етапів: підготовка, виявлення, аналіз, реагування та післядія. Кожен з цих етапів має свої методи та інструменти, такі як форензика, моніторинг і аналіз логів, які дозволяють ефективно ідентифікувати причини та наслідки інцидентів.

Порівняння різних підходів до розслідування інцидентів показало, що і реактивні, і превентивні методи мають свої переваги. Реактивні методи дозволяють швидко реагувати на вже виявлені інциденти, тоді як превентивні підходи спрямовані на запобігання інцидентам через аналіз потенційних загроз і вразливостей. Нові технології та інструменти, такі як штучний інтелект і машинне навчання, значно підвищують ефективність розслідувань, забезпечуючи швидший та точніший аналіз даних. Документування результатів розслідувань є важливим аспектом, що забезпечує можливість аналізу минулих інцидентів і використання отриманого досвіду для покращення майбутніх процедур.

Практичні приклади успішного впровадження методів розслідування свідчать про те, що організації, які інвестують у сучасні технології та навчання персоналу, досягають значного підвищення рівня інформаційної безпеки. Рекомендації щодо покращення організації розслідування інцидентів включають розробку стратегій для вдосконалення процедур розслідування, впровадження нових технологій та інструментів, а також заходів щодо підвищення кваліфікації персоналу. Використання методик організації розслідування інцидентів при управлінні інформаційною безпекою є ефективним підходом, що дозволяє

організаціям більш успішно протистояти загрозам та забезпечувати захист своїх інформаційних ресурсів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бондаренко Д. В. Основи реагування на інциденти інформаційної безпеки : навч. посіб. 2012.

2. Голубів В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навч. посібник / За заг. ред. доктора юридичних наук, професора Р. А. Калюжного. Запоріжжя: ГУ "ЗІДМУ", 2002. 292 с.

3. Розслідування інцидентів інформаційної безпеки. Сучасний захист інформації. 2015. № 4.

4. Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. [Електронний ресурс] – 2009. – 143 с. – Режим доступу: www.isofts.kiev.ua

5. Стахів О. Проведення оцінки персоналу на підприємстві з метою стимулювання працівників до підвищення кваліфікації. *Україна: аспекти праці*. 2007. № 1. С. 29–35.

6. Управління інцидентами інформаційної безпеки. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2019. Вип. 1(38).

7. A Model for Afghanistan’s Cyber Security Incident Response Team / I. Jalal et al. *International Journal on Advanced Science, Engineering and Information Technology*. 2018. Vol. 8, no. 6. P. 2620. URL: https://doi.org/10.18517/ijaseit.8.6.6692

8. Aby A. Top 12 incident management tools for 2024. Hatica. URL: https://www.hatica.io/blog/incident-management-tools/

9. An Organizational Psychology Perspective to Examining Computer Security Incident Response Teams / T. R. Chen et al. *IEEE Security & Privacy*. 2014. Vol. 12, no. 5. P. 61–67. URL: https://doi.org/10.1109/msp.2014.85

10. Anđelski H., Đerković V., Kondić U. Place and role of information security: Information security management model: For owners information.

Zdravstvena zastita. 2011. Vol. 40, no. 6. P. 28–33. URL: https://doi.org/10.5937/zz1102028a

11. Alonzo R. J. Electrical incident investigation procedures. *IEEE Region 5. 2003 Annual Technical Conference. Conference Record. Papers Presented at the 203 Annual Meeting*, New Orleans, LA, USA. URL: https://doi.org/10.1109/reg5.2003.1199711

12. Balzacq T., Cavelty M. D. A theory of actor-network for cyber-security. *European Journal of International Security*. 2016. Vol. 1, no. 2. P. 176–198. URL: https://doi.org/10.1017/eis.2016.8

13. Bhaskar R. A Proposed Integrated Framework for Coordinating Computer Security Incident Response Team. *Journal of Information Privacy and Security*. 2005. Vol. 1, no. 3. P. 3–17. URL: https://doi.org/10.1080/15536548.2005.10855771

14. Computer Security Incident Response Team Development and Evolution / R. Ruefle et al. *IEEE Security & Privacy*. 2014. Vol. 12, no. 5. P. 16–26. URL: https://doi.org/10.1109/msp.2014.89

15. Cooper S. The best incident response tools. Comparitech. URL: https://www.comparitech.com/net-admin/incident-response-tools/

16. Crowd Sensing Intelligence for ITS: Participants, Methods, and Stages / Y. Zhao et al. IEEE Transactions on Intelligent Vehicles. 2023. P. 1–6. URL: https://doi.org/10.1109/tiv.2023.3284046

17. Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry / A. Geil et al. *International Food and Agribusiness Management Review*. 2018. Vol. 21, no. 3. P. 317–334. URL: https://doi.org/10.22434/ifamr2017.0045

18. Design principles for critical incident response systems / R. Chen et al. *Information Systems and e-Business Management*. 2007. Vol. 5, no. 3. P. 201–227. URL: https://doi.org/10.1007/s10257-007-0046-0

19. Dekić M. Incident response as a key factor of defense. *Tehnika*. 2020. Vol. 75, no. 6. P. 809–813. URL: https://doi.org/10.5937/tehnika2006809d

20. Distributed Security Framework for Reliable Threat Intelligence Sharing / D. Preuveneers et al. *Security and Communication Networks*. 2020. Vol. 2020. P. 1–15. URL: https://doi.org/10.1155/2020/8833765

21. Hamilton K. T., Herson M. R. Skin bank development and critical incident response. *Cell and Tissue Banking*. 2010. Vol. 12, no. 2. P. 147–151. URL: https://doi.org/10.1007/s10561-010-9181-9

22. Horne B. On Computer Security Incident Response Teams. *IEEE Security & Privacy*. 2014. Vol. 12, no. 5. P. 13–15. URL: https://doi.org/10.1109/msp.2014.96

23. Information Security Incident Management. *Information Security*. 2006. P. 195–198. URL: https://doi.org/10.1201/9781420013412.ch15

24. Improving Forensic Triage Efficiency through Cyber Threat Intelligence / N. Serketzis et al. *Future Internet*. 2019. Vol. 11, no. 7. P. 162. URL: https://doi.org/10.3390/fi11070162

25. Integrating tools for an effective testing of connected and automated vehicles technologies / L. Pariota et al. *IET Intelligent Transport Systems*. 2020. Vol. 14, no. 9. P. 1025–1033. URL: https://doi.org/10.1049/iet-its.2019.0678

26. Investigating Subtle Lithologic Information in Forested Regions of Northwestern Ontario Using Field and Remote Sensing Approaches / R. Bell et al. *Canadian Journal of Remote Sensing*. 1991. Vol. 17, no. 2. P. 85–96. URL: https://doi.org/10.1080/07038992.1991.10855283

27. Johansen G. Digital Forensics and Incident Response: Incident Response Tools and Techniques for Effective Cyber Threat Response. Packt Publishing, Limited, 2022.

28. Kent K., Chevalier S., Grance T., Dang H. *Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology* (NIST). Publ. 800-86. 2006.

29. Kosiński J., Gontarz T., Kośla R. Cybersecurity and the Handling of Cyber Incidents. *Internal Security*. 2019. Vol. 10, no. 2. P. 107–128. URL: https://doi.org/10.5604/01.3001.0013.4219

30. Kukla C. D., Morse R. S. Designing Effective Systems: A Tool Approach. *Usability: Turning Technologies into Tools*. 1993. URL: https://doi.org/10.1093/oso/9780195075106.003.0006

31. Mitropoulos S., Patsos D., Douligeris C. Incident response requirements for distributed security information management systems. *Information Management & Computer Security*. 2007. Vol. 15, no. 3. P. 226–240. URL: https://doi.org/10.1108/09685220710759568

32. On the Improvement of Grid Resource Utilization: Preventive and Reactive Rescheduling Approaches / L. Tomás et al. *Journal of Grid Computing*. 2012. Vol. 10, no. 3. P. 475–499. URL: https://doi.org/10.1007/s10723-012-9226-3

33. Polotai O. I. Використання комп'ютерної криміналістики для забезпечення ефективного розслідування інцидентів інформаційної та кібербезпеки. *Bulletin of Lviv State University of Life Safety*. 2023. Т. 28. С. 73–80. URL: https://doi.org/10.32447/20784643.28.2023.07

34. Poetiray I. F. Z., Salman M. Information security incident management using iso 27035 standard. *Gema Wiralodra*. 2023. Vol. 14, no. 3. P. 168–178. URL: https://doi.org/10.31943/gw.v14i3.487

35. Positive Technologies. Results of cybersecurity incident investigations in 2021–2023. ptsecurity.com. URL: https://www.ptsecurity.com/ww-en/analytics/results-of-cybersecurity-incident-investigations-in-2021-2023/

36. Sundaram A. Understanding and Protecting Yourself against Threats in the Internet. *Asian Social Science*. 2017. Vol. 13, no. 12. P. 201. URL: https://doi.org/10.5539/ass.v13n12p201

37. S. Nallusamy et al., S. N. e. a. ,. Investigation Study on Effective Tools for Conscription of Various Industrial Applications. *International Journal of Mechanical and Production Engineering Research and Development*. 2018. Vol. 8, no. 1. P. 1221–1230. URL: https://doi.org/10.24247/ijmperdfeb2018143

38. Scenario-based training to improve nursing staff knowledge and competence in diabetes care / J. J. Kwan et al. *Diabetes Research and Clinical Practice*. 2016. Vol. 120. P. S172. URL: https://doi.org/10.1016/s0168-8227(16)31379-1

39. Scaglione B. J. Incident and Event Investigation. *Security Management for Healthcare*. 2019. P. 77–86. URL: https://doi.org/10.4324/9780429023705-5

40. Shen Y.-T., Lin F., Rohm C. E. T. A Framework for Enterprise Security Architecture and Its Application in Information Security Incident Management. *Communications of the IIMA*. 2014. Vol. 9, no. 4. URL: https://doi.org/10.58729/1941-6687.1118

41. Sterneckert A. B. Incident Response Management. *Information Security Management*. 2019. P. 855–871. URL: https://doi.org/10.1201/9781351073547-57

42. Training residents in medical incident report writing to improve incident investigation quality and efficiency enables accurate fact gathering / Y.Maeda et al. *Applied Ergonomics*. 2022. Vol. 102. P. 103770. URL: https://doi.org/10.1016/j.apergo.2022.103770

43. Villegas-Ch. W., Ortiz-Garces I., Sánchez-Viteri S. Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus. *Computers*. 2021. Vol. 10, no. 8. P. 102. URL: https://doi.org/10.3390/computers10080102

44. Vucinic D. Management of Security Processes in Information Technologies. *American Journal of Management Science and Engineering*. 2021. Vol. 6, no. 6. P. 224. URL: https://doi.org/10.11648/j.ajmse.20210606.17

45. Zheng R., Lu W., Xu S. Preventive and Reactive Cyber Defense Dynamics Is Globally Stable. *IEEE Transactions on Network Science and Engineering*. 2018. Vol. 5, no. 2. P. 156–170. URL: https://doi.org/10.1109/tnse.2017.2734904

ДОДАТКИ

Додаток А

Ключові стратегії для покращення розслідувань інцидентів кібербезпеки

№	Ключова стратегія	Опис	Приклади використання та інструменти
1	Безперервний моніторинг	Збір і аналіз даних з різних джерел для виявлення аномалій та загроз у реальному часі.	Інструменти SIEM, рішення для моніторингу мережевого трафіку.
2	Пріоритизація інцидентів	Визначення пріоритетів інцидентів на основі їх впливу для ефективного розподілу ресурсів.	Платформи управління інцидентами, оцінка ризиків на основі бізнес-імпакту.
3	Правила Sigma	Стандартизовані правила для виявлення загроз на різних платформах і системах.	Використання в SIEM-системах, інтеграція з інструментами безпеки для автоматизації виявлення загроз.
4	Збір та зберігання доказів	Централізоване зберігання доказів для їх аналізу та юридичного використання.	Системи управління цифровими доказами, використання шифрування для захисту доказів.
5	Хмарна документація	Використання хмарних рішень для документації та координації роботи команд.	Платформи для спільної роботи, хмарні сервіси для зберігання та обміну даними.
6	Штучний інтелект і машинне навчання	Автоматизація аналізу та виявлення загроз за допомогою штучного інтелекту та машинного навчання.	Використання інструментів для аналізу даних і прогнозування загроз, моделі МН для аналізу мережевого трафіку.
7	Інструменти криміналістичного аналізу	Глибокий аналіз векторів атак для розуміння методів зловмисників.	Форензика пам’яті, аналіз дисків, глибокий аналіз мережевого трафіку.
8	Інтеграція розвідданих про загрози	Використання даних про загрози для покращення розслідувань та захисту.	Платформи для розвідки загроз, об’єднання зовнішніх даних із внутрішніми для створення повної картини загроз.

Додаток Б

Шкідливе програмне забезпечення, що використовується в APT-атаках

№	Назва шкідливого ПЗ	Опис
1	App_global	Шкідливе ПЗ для отримання доступу до внутрішніх мереж та даних.
2	Даксін	Високотехнологічний бекдор для тривалого доступу.
3	ФейсФіш	Програма для крадіжки облікових даних.
4	Msdaprst Бекдор	Бекдор для віддаленого управління скомпрометованими системами.
5	ShadowPad	Потужний інструмент для віддаленого доступу і виконання команд.
6	Лейозавр	Використовується для прихованого віддаленого доступу.
7	Собака-приманка	Шкідливе ПЗ, що імітує легальні програми.
8	Фасоль PAT	Програма для віддаленого доступу до комп'ютерів (Remote Access Trojan).
9	Технологія MSMRAT	Інструмент для тривалого віддаленого доступу і моніторингу.
10	Тротуарі	Шкідливе ПЗ для збору даних і встановлення контролю над системами.
11	BeaconLoader	Інструмент для завантаження додаткового шкідливого ПЗ.
12	DeedRAT	Програма для прихованого управління системами.
13	Gh0st	Бекдор, що забезпечує повний контроль над системою.
14	owowa	Шкідливе ПЗ для викрадення облікових даних з поштових серверів.
15	ЛІЧИЛЬНИК	Інструмент для збору інформації про систему.
16	Бізонал	Використовується для довготривалого доступу до внутрішніх мереж.
17	Інструмент DiskTool	Шкідливе ПЗ для управління та маніпулювання даними на дисках.
18	IP He1per (PingPull)	Програма для виконання команд на віддаленому сервері.
19	Плагін (PlugX)	Багатофункціональний бекдор для управління комп'ютерами.
20	TaskMasters Backdoor	Інструмент для віддаленого доступу та збору інформації.
21	CobInt	Використовується для збору інформації про системи та мережі.

22	DNSep	Шкідливе ПЗ для маніпуляцій з DNS-запитами.
23	Кіцуне	Програма для маскування активності зловмисника.
24	ProjC	Використовується для встановлення контролю над системами.
25	TaskMasters Backdoor PowerShell	Інструмент для виконання команд на віддалених системах через PowerShell.
26	CotxRat	Програма для віддаленого доступу до систем.
27	DonutHole	Шкідливе ПЗ для прихованого збору даних.
28	Матадор	Використовується для виконання команд на скомпрометованих системах.
29	PwShell	Інструмент для управління системами через оболонку PowerShell.
30	TgRAT	Програма для віддаленого доступу та збору даних.
31	Темний пульсар (2017)	Бекдор для тривалого доступу до систем.
32	Doorme	Шкідливе ПЗ для віддаленого управління системами.
33	Мікроцин	Використовується для прихованого збору інформації.
34	Remshell (Ремшелл)	Інструмент для віддаленого доступу до систем.
35	ThreatNeedle (Голка загрози)	Шкідливе ПЗ для збору даних та виконання команд на скомпрометованих системах.
36	TinyFluff (Крихітний пух)	Використовується для збору інформації з мережі.
37	TinyNode (Вузол TinyNode)	Шкідливе ПЗ для прихованого збору даних.
38	ТокіоХ	Програма для віддаленого доступу до мереж та збору інформації.
39	Войдоур	Інструмент для збору та передачі даних на віддалені сервери.
40	XDSpy	Використовується для збору інформації з корпоративних мереж.