**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 РЕАГУВАННЯ НА ІНЦИДЕНТИ 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*

_____ Кірил СІЙЧУК
*(підпис)* *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Кірил СІЙЧУК
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЯКИМЕНКО
*К.в.н., доцент* Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
*Д.т.н., професор* 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

Сійчуку Кірилу Ігоровичу
*(прізвище, ім’я, по батькові здобувача)*

1. Тема кваліфікаційної роботи “Організація реагування на інциденти 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 реагування на інциденти інформаційної безпеки.
   4.2. Дослідити практичний досвід реагування на інциденти.
   4.3. Розробити рекомендації щодо покращення організації реагування на інциденти 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 реагування на інциденти інформаційної безпеки | 08.04.2024 | |
| 4. | Дослідження практичного досвіду реагування на інциденти. | 22.04.2024 | |
| 5. | Розробка рекомендацій щодо покращення організації реагування на інциденти 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 ЕК. | __.06.2024 | |

Здобувач вищої освіти _____ Кірил СІЙЧУК

*(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 Сійчук К.І. 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 реагування на інциденти інформаційної безпеки”

Кваліфікаційна робота і рецензія додаються.

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

**Висновок керівника кваліфікаційної роботи**

Здобувач СІЙЧУК Кірил у кваліфікаційній роботі проаналізував особливості реагування на інциденти при управлінні інформаційною безпекою підприємства, дослідив основні методи та процедури виявлення інцидентів на підприємстві, вивчив найкращі практики та висновки з практичного досвіду ефективності використання процедур реагування на інциденти інформаційної безпеки, розробив практичні рекомендації за темою дослідження.

СІЙЧУК Кірил 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 конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача СІЙЧУКА Кірила на оцінку “відмінно” 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 Сійчук К.І. 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 СІЙЧУКА Кірила
на тему “ Організація реагування на інциденти інформаційної безпеки”

**Актуальність.**

На сьогодні в міжнародній практиці представлено значний спектр нормативних документів, які регламентують питання управління інцидентами інформаційної безпеки. Зокрема, в рамках стандарту ISO/IEC 27001 представлені загальні вимоги до побудови системи управління інформаційною безпекою, які в тому числі відносяться і до процесів управління інцидентами. В контексті забезпечення інформаційної безпеки визначальним є комплексний підхід щодо виявлення інцидентів інформаційної безпеки , реагування на них, а також проведення аналізу інцидентів для того, щоб спланувати превентивні заходи захисту та вдосконалити процес забезпечення інформаційної безпеки в цілому. Важливе значення в сфері управління безпекою наділяється організації процесу реагування на інциденти, що враховує аналіз загроз та пошук вразливостей, проведення аналізу та аудиту журналів подій, що обумовлені функціонуванням інформаційної інфраструктури. Аналіз і оцінка ефективності реагування на інциденти є критичними аспектами для постійного вдосконалення інших систем управління в сфері безпеки. та їх адаптації до змін у загрозах. Регулярне тестування і аудит процесів реагування допомагають виявити слабкі місця та впровадити необхідні покращення для підвищення рівня безпеки інформації і інформаційної безпеки організації в цілому.

**Позитивні сторони.**

Кваліфікаційна робота охоплює важливу та актуальну тему, пов'язану з організацією реагування на інциденти інформаційної безпеки, що відображає значущість цієї проблеми у сучасному цифровому світі. Кваліфікаційна робота демонструє достатній аналіз застосовуваних методик та підходів до організації реагування на інциденти. Вступ та висновки роблять роботу добре організованою та логічно зв'язаною. Сформовані рекомендації щодо покращення процесів реагування на інциденти є важливим аспектом дослідницької роботи, що відображає сучасні методичні підходи у галузі інформаційної безпеки.

**Недоліки.**

Хоча робота достатньо структурована, варто було розглянути можливість більш детального аналізу окремих методів і процедур виявлення інцидентів та їхнього порівняння, щоб надати глибше розуміння вибору конкретних методичних підходів покращення окремих процедур реагування на інциденти. Це дозволить визначити найбільш ефективні та відповідні методи реагування на інциденти для різних типів підприємств.

Рекомендацією для майбутнього дослідження може бути розгляд можливості застосування методики ефективного виявлення та аналізу інцидентів в управлінні інформаційною безпекою на конкретних прикладах чи в реальних умовах діяльності підприємств. Такий підхід дозволить оцінити практичну ефективність методів та адаптувати їх до специфічних потреб і умов різних підприємств , забезпечуючи максимальну ефективність реагування на інциденти інформаційної безпеки.

**Висновок:** Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач СІЙЧУК Кірил заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Галина ГАЙДУР _
д.т.н., професор *підпис* Ім’я, ПРІЗВИЩЕ

# РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню процесів реагування інцидентами інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 11 рисунків, висновків і списку використаних джерел із 49 найменувань. Загальний обсяг роботи становить 70 аркушів, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

***Метою роботи*** є організація реагування на інциденти інформаційної безпеки.

***Об'єктом дослідження*** є процеси реагування інцидентами інформаційної безпеки.

***Предмет дослідження*** – особливості 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 основні теоретичні аспекти реагування на інциденти інформаційної безпеки, досліджено практичний досвід реагування на інциденти; розроблено рекомендації щодо покращення організації реагування на інциденти інформаційної безпеки.

***Галузь застосування.*** Розроблені підходи можуть бути використані при організації реагування на інциденти у контексті інформаційної безпеки.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ОРГАНІЗАЦІЯ РЕАГУВАННЯ НА ІНЦИДЕНТИ, ЕТАПИ ТА ПРИНЦИПИ РЕАГУВАННЯ НА ІНЦИДЕНТИ, МЕТОДИКИ ОРГАНІЗАЦІЇ РЕАГУВАННЯ.

# ABSTRACT

The qualification work is devoted to the study of information security incident response processes. The work consists of an introduction, three chapters containing 11 figures, conclusions and the list of references containing 49 items. The total volume of the work is 70 pages, of which 6 pages are occupied by the list of abbreviations and the list of references.

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

***The object the study*** are processes of responding to information security incidents.

***The subject of the study*** is the peculiarities of responding to 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 responding to information security incidents, examines the practical experience of responding to incidents; develops recommendations for improving the organization of response to information security incidents.

***Field of application.*** The developed approaches can be used in incident response organizing in the context of information security.

Keywords: INFORMATION SECURITY, INFORMATION SECURITY INCIDENTS, ORGANIZATION OF INCIDENT RESPONSE, STAGES AND PRINCIPLES OF INCIDENT RESPONSE, METHODS OF RESPONSE ORGANIZING.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

| | | |
|---|---|---|
| ІКТ | – | Інформаційно-комунікаційні технології |
| IDS | – | Система виявлення вторгнень |
| IPS | – | Система попередження про вторгнення |
| SIEM | – | Security Information and Event Management |
| МКЧХ | – | Міжнародний комітет Червоного Хреста |
| IR | – | Реагування на інцидент |
| IOC | – | Індикатори компрометації |
| EDR | – | Рішення для виявлення та реагування на кінцевих точках |

# ВСТУП

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

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

***Мета роботи*** полягає у організації реагування на інциденти інформаційної безпеки..

***Об'єкт дослідження –*** процеси реагування інцидентами інформаційної безпеки.

***Предмет дослідження*** – особливості реагування на інциденти інформаційної безпеки.

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

1. Проаналізувати теоретичні аспекти реагування на інциденти інформаційної безпеки.

2. Дослідити практичний досвід реагування на інциденти.

3. Розробити рекомендації щодо покращення організації 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 основні теоретичні аспекти реагування на інциденти інформаційної безпеки, досліджено практичний досвід реагування на інциденти; розроблено рекомендації щодо покращення організації

реагування на інциденти інформаційної безпеки.

***Практичне значення одержаних результатів.*** Застосування напрацювань дасть змогу здійснити правильну оцінку забезпечення безпеки інформації на підприємстві. Результати дослідження можуть допомогти оптимізувати систему реагування на інциденти інформаційної безпеки, спираючись на оцінку наявних методів та рекомендації 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 РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Теоретичні аспекти реагування на інциденти інформаційної безпеки є ключовими складовими сучасної кібербезпеки, що визначають ефективність захисту інформаційних ресурсів та мінімізацію потенційних втрат від кіберзагроз. В умовах стрімкого розвитку інформаційних технологій та зростання складності кібернетичних атак, розробка науково обґрунтованих підходів до управління інцидентами інформаційної безпеки набуває особливого значення.

Дослідження в цій галузі фокусуються на створенні теоретичних моделей, методів і алгоритмів, що забезпечують своєчасне виявлення, аналіз, реагування та відновлення після інцидентів. Зокрема, значну увагу приділено питанням класифікації інцидентів, оцінки ризиків, визначення критичних точок інфраструктури, а також розробці стратегій і процедур для оперативного реагування на загрози. Важливими елементами є також міждисциплінарний підхід та інтеграція знань з різних галузей, таких як комп'ютерні науки, криптографія, менеджмент та правознавство.

## 1.1 Сутність та класифікація інцидентів інформаційної безпеки

Інциденти інформаційної безпеки є невід’ємною складовою ризиків, пов’язаних з використанням інформаційно-комунікаційних технологій (ІКТ). Вони можуть проявлятися у вигляді порушень конфіденційності, цілісності та доступності інформації, що спричиняють негативні наслідки для організацій, державних установ та приватних осіб. Поняття інциденту інформаційної безпеки охоплює будь-які події або серії подій, які негативно впливають на стан захищеності інформаційних ресурсів.

Наукові підходи до визначення сутності інцидентів інформаційної безпеки включають кілька ключових аспектів (рис. 1.1):

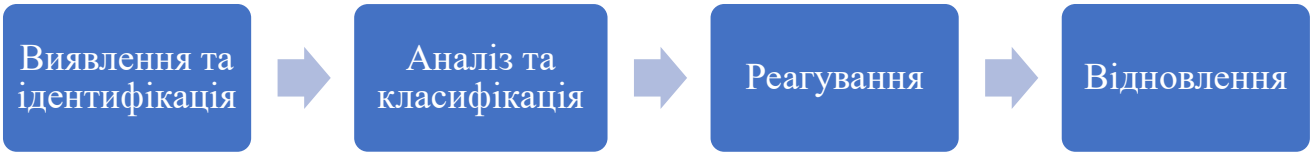


Рис. 1.1 Наукові підходи до визначення сутності інцидентів інформаційної безпеки

Виявлення та ідентифікація – процес визначення факту виникнення інциденту, що включає виявлення аномальної активності, яка може свідчити про порушення безпеки.

Виявлення та ідентифікація інцидентів інформаційної безпеки є критичними етапами в управлінні кібербезпекою, оскільки вони визначають ефективність усіх наступних заходів щодо реагування та відновлення. Ці етапи вимагають застосування комплексного підходу, що включає використання як технічних засобів, так і організаційних заходів [1].

Виявлення інцидентів інформаційної безпеки полягає у своєчасному виявленні аномальних активностей або подій, які можуть свідчити про порушення безпеки. Це завдання є складним і багатогранним, оскільки кіберзагрози можуть мати різні форми і використовувати численні техніки для уникнення виявлення. Ефективне виявлення ґрунтується на кількох ключових компонентах:

Постійний моніторинг мережевого трафіку дозволяє виявляти підозрілі активності, такі як незвичні обсяги даних, спроби несанкціонованого доступу або аномальні шаблони використання мережі. Для цього використовуються системи виявлення вторгнень (IDS) та системи попередження про вторгнення (IPS).

Збирання і аналіз лог-файлів з різних компонентів інформаційної системи (серверів, мережевих пристроїв, додатків) дозволяє виявляти аномалії та підозрілі події. Засоби для аналізу логів, такі як SIEM (Security Information and

Event Management) системи, допомагають централізовано збирати, аналізувати та корелювати дані з різних джерел.

Використання сучасних антивірусних рішень, що здатні виявляти відомі шкідливі програми та їх варіанти, є важливим елементом захисту. Антивірусні програми повинні регулярно оновлювати свої бази даних для ефективного виявлення нових загроз.

Використання методів машинного навчання та штучного інтелекту для аналізу поведінки користувачів та системних компонентів допомагає виявляти аномальні дії, що можуть свідчити про інциденти безпеки. Це дозволяє ідентифікувати загрози, що не можуть бути виявлені традиційними методами.

Після виявлення підозрілої активності необхідно провести ідентифікацію інциденту, щоб визначити його характер, джерело та можливі наслідки. Ідентифікація включає кілька важливих етапів:

Визначення типу загрози (наприклад, вірус, атака типу «відмова в обслуговуванні», спроба фішингу) допомагає вибрати правильну стратегію реагування. Це передбачає використання баз даних відомих загроз та вразливостей [2].

Ідентифікація джерела загрози, що може включати аналіз IP-адрес, географічного розташування та інших метаданих, дозволяє зрозуміти, хто стоїть за атакою, та вжити відповідних заходів.

Визначення потенційних наслідків інциденту для інформаційної системи та бізнес-процесів організації є важливим для пріоритезації заходів з реагування. Це включає оцінку втрат конфіденційності, цілісності та доступності даних.

Зв'язування різних подій між собою для виявлення повного масштабу інциденту. Це допомагає зрозуміти, чи є виявлені події частиною більш широкої атаки.

Перевірка та підтвердження того, що виявлені аномалії дійсно є інцидентами інформаційної безпеки, а не хибними спрацюваннями. Це може включати ручну перевірку експертами з безпеки.

Процес виявлення та ідентифікації інцидентів інформаційної безпеки є фундаментом для всіх подальших заходів щодо управління кібербезпекою. Від його ефективності залежить здатність організації своєчасно реагувати на загрози, мінімізувати збитки та забезпечити безперервність бізнес-процесів. У сучасних умовах, коли кількість та складність кіберзагроз постійно зростають, інтеграція новітніх технологій моніторингу, аналізу та ідентифікації є необхідною для побудови надійної системи кібербезпеки.

Аналіз та класифікація – визначення характеру, джерел та можливих наслідків інциденту, а також його класифікація для подальшого реагування.

Аналіз та класифікація інцидентів інформаційної безпеки є критично важливими процесами, які дозволяють ефективно керувати кіберзагрозами та забезпечувати стабільне функціонування інформаційних систем. У контексті стрімкого розвитку технологій та збільшення кількості кібератак, ці процеси набувають все більшого значення для організацій усіх розмірів та галузей [3].

Аналіз інцидентів інформаційної безпеки розпочинається з виявлення аномальної активності, що може свідчити про наявність загрози. На цьому етапі застосовуються різноманітні технічні засоби та методи, такі як системи виявлення вторгнень (IDS), моніторинг мережевого трафіку та аналіз логів. Основне завдання полягає у своєчасному виявленні інциденту, що дозволяє мінімізувати можливі збитки.

Після виявлення інциденту, важливо провести його детальний аналіз. Цей процес включає ідентифікацію джерела загрози, визначення методів, які були використані зловмисниками, а також оцінку масштабу та потенційних наслідків інциденту. Для цього використовуються різноманітні інструменти та методики, такі як форензичний аналіз, аналіз зловмисного програмного забезпечення та зворотне проектування атак.

Класифікація інцидентів є наступним важливим етапом, який дозволяє систематизувати виявлені загрози та визначити оптимальні стратегії реагування. Класифікація базується на різних критеріях, що охоплюють характер загрози, її джерело, спосіб реалізації та наслідки. Вони зображені на рис. 1.2.


Рис. 1.2 Критерії класифікації інцидентів інформаційної безпеки

Одним з ключових аспектів класифікації є характер загрози. Зокрема, інциденти можуть бути спричинені зовнішніми або внутрішніми суб'єктами. Зовнішні загрози, як правило, походять від хакерів, конкурентних організацій або навіть державних структур, які прагнуть отримати несанкціонований доступ до інформаційних ресурсів. Внутрішні загрози, у свою чергу, можуть бути спричинені як навмисними діями співробітників (наприклад, крадіжка даних), так і ненавмисними (наприклад, помилки або недбалість) [4].

Джерело загрози також є важливим критерієм класифікації. Технічні загрози включають вразливості в програмному або апаратному забезпеченні, які можуть бути експлуатовані зловмисниками для отримання доступу до системи. Соціальні загрози базуються на методах соціальної інженерії, де нападники використовують психологічні маніпуляції для отримання конфіденційної інформації.

Спосіб реалізації загрози визначає, чи є атака пасивною чи активною. Пасивні атаки, як правило, не втручаються в роботу системи, а лише спостерігають або збирають дані. Прикладом може бути перехоплення мережевого трафіку. Активні атаки, навпаки, передбачають активне втручання в

роботу системи, зміну даних або порушення функціонування (наприклад, атаки типу DoS) [5].

Наслідки інцидентів також є важливим критерієм класифікації. Вони можуть включати порушення конфіденційності (розголошення конфіденційної інформації), порушення цілісності (несанкціонована зміна або видалення даних) та порушення доступності (втрата доступу до інформаційних ресурсів).

Аналіз та класифікація інцидентів інформаційної безпеки є комплексними процесами, що вимагають інтеграції знань з різних галузей та використання сучасних технологій. Вони дозволяють не лише виявляти та ідентифікувати загрози, але й розробляти ефективні стратегії реагування, спрямовані на мінімізацію збитків та забезпечення стійкості інформаційних систем. У світі, де інформаційні технології відіграють ключову роль, здатність організацій ефективно управляти інцидентами інформаційної безпеки стає вирішальним фактором їхньої успішності та конкурентоспроможності.

Реагування – набір заходів, спрямованих на нейтралізацію загрози, мінімізацію збитків та відновлення нормального функціонування систем.

Реагування на інциденти інформаційної безпеки є невід’ємною складовою сучасної стратегії кібербезпеки, оскільки жодна система не може бути абсолютно захищеною від загроз. Навіть найсучасніші засоби захисту можуть виявитися недостатніми перед новими, ще невідомими методами атак. Тому ефективне реагування на інциденти стає ключовим фактором у зменшенні шкоди від кібератак і відновленні нормального функціонування систем [6].

Реагування на інциденти інформаційної безпеки передбачає сукупність заходів, спрямованих на виявлення, оцінку, нейтралізацію та ліквідацію наслідків інцидентів, що загрожують безпеці інформаційних систем. Цей процес включає декілька етапів.

На етапі виявлення інциденту використовуються різноманітні інструменти моніторингу, такі як системи виявлення вторгнень (IDS), антивірусні програми, засоби аналізу мережевого трафіку. Важливо виявити інцидент на ранній стадії, щоб мінімізувати потенційну шкоду.

Після виявлення інциденту необхідно провести його оцінку. Це включає визначення джерела загрози, її природи, ступеня впливу та можливих наслідків. Класифікація інциденту дозволяє зрозуміти, наскільки серйозною є загроза і які заходи необхідно вжити для її нейтралізації.

Важливо оперативно інформувати про інцидент усіх зацікавлених сторін – від керівництва організації до відповідальних технічних фахівців. В окремих випадках може бути необхідним також інформування партнерів, клієнтів чи навіть громадськості [7].

Нейтралізація загрози – це основний етап реагування, що передбачає вжиття заходів для зупинки атаки, видалення шкідливого програмного забезпечення, закриття вразливостей та інших дій, спрямованих на припинення інциденту. Важливо діяти швидко та рішуче, щоб звести до мінімуму негативні наслідки.

Після нейтралізації загрози необхідно відновити нормальну роботу інформаційних систем. Це може включати відновлення даних із резервних копій, перевірку цілісності систем та їх повторну перевірку на наявність вразливостей.

Завершальний етап реагування передбачає детальний аналіз інциденту з метою виявлення його причин та вжиття заходів для запобігання подібним випадкам у майбутньому. Цей процес включає підготовку звітів, перегляд та оновлення політик безпеки, навчання персоналу.

Ефективне реагування на інциденти інформаційної безпеки має критичне значення з кількох причин. По-перше, швидке реагування дозволяє зменшити масштаб шкоди, яку може завдати кібератака. По-друге, воно сприяє швидкому відновленню нормальної роботи систем, що мінімізує фінансові втрати та зниження продуктивності. По-третє, належне реагування підвищує довіру з боку клієнтів та партнерів, оскільки демонструє здатність організації ефективно захищати свої інформаційні ресурси.

Реагування на інциденти інформаційної безпеки стикається з низкою викликів. Одним з основних є брак кваліфікованих фахівців у галузі кібербезпеки. Це вимагає постійного навчання та підвищення кваліфікації

персоналу. Ще одним викликом є швидка еволюція кіберзагроз, що вимагає від організацій постійно оновлювати свої методи та засоби захисту.

На перспективу важливим напрямом є впровадження автоматизованих систем реагування, що базуються на штучному інтелекті та машинному навчанні. Вони дозволяють швидше виявляти та нейтралізувати загрози, зменшуючи навантаження на фахівців та підвищуючи ефективність кіберзахисту.

Відновлення – дії з повернення інформаційних систем до стану, що передував інциденту, а також аналіз інциденту з метою запобігання подібним випадкам у майбутньому [8].

Після виявлення та аналізу інциденту інформаційної безпеки настає важливий етап відновлення, спрямований на повернення інформаційних систем до нормального функціонування та мінімізацію збитків, які можуть виникнути в результаті атаки. Цей процес стикається з рядом викликів, таких як складність аналізу наслідків, необхідність швидкого відновлення та гарантування безпеки під час відновлювальних робіт.

Одним з головних викликів відновлення після інцидентів інформаційної безпеки є збереження критично важливої інформації та відновлення її доступності для користувачів. У разі атак на інформаційні системи можуть бути втрачені або пошкоджені дані, що може спричинити серйозні фінансові та репутаційні збитки для організації. Крім того, важливо гарантувати безпеку під час відновлення, щоб уникнути повторного вторгнення або інших подібних інцидентів.

Ще одним важливим аспектом є швидкість відновлення. У сучасному світі інформаційних технологій, де кількість та складність кібератак постійно зростають, кожна хвилина простою може призвести до серйозних втрат для бізнесу. Тому важливо мати ефективні процедури та технічні засоби для швидкого відновлення після інциденту.

Для успішного відновлення після інциденту інформаційної безпеки важливо мати чітку стратегію, яка включає в себе кілька ключових етапів, що зображені на рис. 1.3.


Рис. 1.3. Ключові етапи успішного відновлення після інциденту інформаційної безпеки

Першим кроком є проведення детального аналізу наслідків інциденту, визначення обсягу пошкоджень та пріоритетів відновлення. Важливо визначити, які системи або дані потребують найбільшого пріоритету для відновлення, щоб мінімізувати вплив на бізнес-процеси [9].

Після визначення пріоритетів необхідно відновити доступність та цілісність даних. Це може включати відновлення резервних копій даних, використання методів реплікації даних та перевірку на наявність вірусів або шкідливого програмного забезпечення.

Після відновлення доступності та цілісності даних важливо забезпечити їхню безпеку. Це може включати використання захисних механізмів, таких як антивірусне програмне забезпечення, системи виявлення вторгнень та шифрування даних.

Після відновлення важливо провести аналіз інциденту та ідентифікувати причини та уроки, які можна вивчити з нього. Це дозволить удосконалити процеси управління інцидентами та зменшити ризики подібних інцидентів у майбутньому. На основі аналізу можна розробити та впровадити вдосконалені стратегії захисту, а також покращити процедури виявлення та реагування на інциденти. Крім того, важливо провести навчання персоналу з питань кібербезпеки, щоб підвищити рівень обізнаності та вміння реагувати на потенційні загрози.

Для ефективного управління інцидентами інформаційної безпеки необхідно мати чітку класифікацію, що дозволяє систематизувати різні типи інцидентів та розробляти відповідні стратегії реагування. Класифікація інцидентів інформаційної безпеки базується на різних критеріях, зокрема на характері загрози, її джерелі, способі реалізації та наслідках.

## 1.2 Методи та процедури виявлення інцидентів

Методи виявлення інцидентів інформаційної безпеки включають в себе різноманітні техніки та інструменти, які використовуються для виявлення аномальних або підозрілих активностей у мережах та системах. Системи і підготовка до виявлення інцидентів зображено на рис. 1.4.

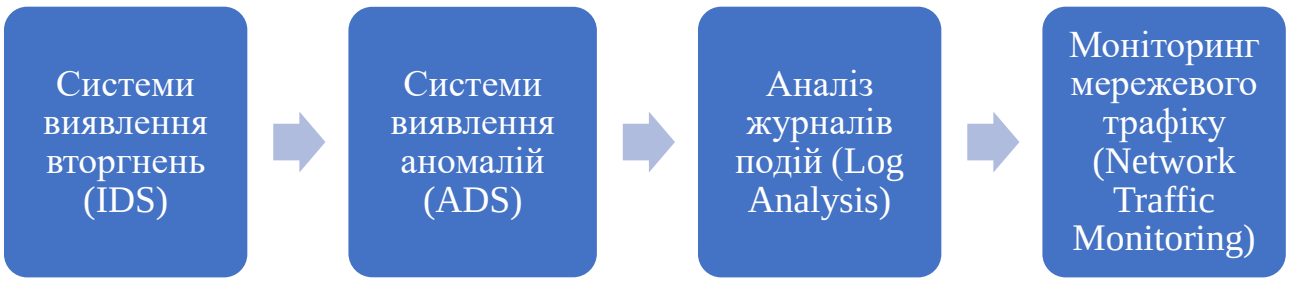


Рис. 1.4 Системи і підготовка до виявлення інцидентів

IDS є програмними або апаратними системами, які моніторять мережевий трафік або активність в інформаційних системах для виявлення аномальних патернів, що можуть свідчити про потенційні загрози. Ці системи можуть виявляти різноманітні види атак, включаючи вторгнення, атаки з використанням вразливостей та інші види кіберзлочинності.

ADS аналізують активність системи для виявлення аномальних патернів, які можуть свідчити про потенційні загрози. Вони базуються на аналізі статистики та використанні машинного навчання для виявлення змін у поведінці системи, які можуть бути індикаторами атаки [10].

Log Analysis включає в себе аналіз журналів подій або логів, які створюються системами та додатками під час їх роботи. Аналіз журналів подій дозволяє виявляти підозрілі або несподівані події, такі як спроби неуспішного входу, незвичні запити до системи тощо.

Network Traffic Monitoring полягає в аналізі мережевого трафіку для виявлення аномальних або незвичних патернів, які можуть свідчити про атаки або несанкціонований доступ.

Процедури виявлення інцидентів інформаційної безпеки включають в себе набір кроків та дій, які слід виконати для ефективного виявлення та реагування на потенційні загрози. Вони зображені на рис. 1.5.

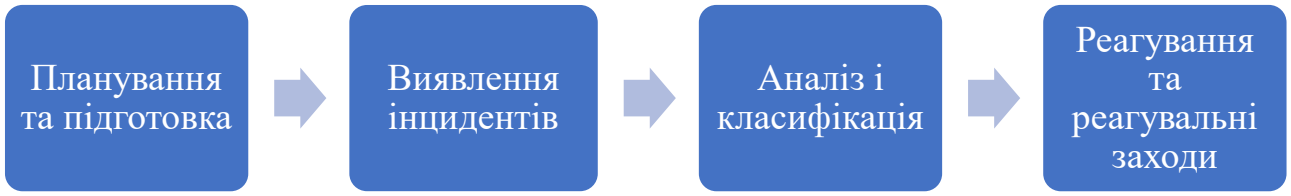


Рис. 1.5. Процедури виявлення інцидентів

Планування та підготовка включає в себе розробку плану виявлення інцидентів, визначення обов'язків та відповідальності персоналу, а також підготовку необхідних інструментів та ресурсів для виявлення та аналізу інцидентів [11].

Виявлення інцидентів використовує різні методи виявлення, такі як системи виявлення вторгнень, аналіз журналів подій та моніторинг мережевого трафіку, для виявлення аномальних активностей або підозрілих патернів.

Після виявлення інциденту проводиться його детальний аналіз та класифікація, що дозволяє визначити характер загрози, її джерело та наслідки.

На етапі реагування та реагувальні заходи приймаються заходи для нейтралізації загрози та мінімізації збитків, включаючи блокування

### 1.3 Техніки та інструменти виявлення інцидентів

Ефективне реагування на інциденти інформаційної безпеки передбачає послідовність етапів, які дозволяють забезпечити швидке та адекватне вирішення ситуації. Етапи реагування на інциденти зображено на рис. 1.6.

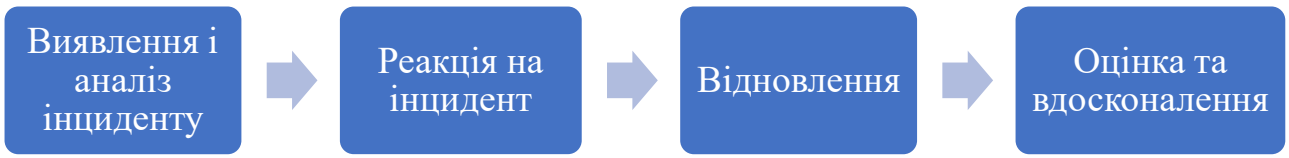


Рис. 1.6. Етапи реагування на інциденти

Першим етапом є виявлення аномальної активності або підозрілих патернів, що можуть свідчити про наявність інциденту. Після виявлення інциденту проводиться його детальний аналіз для визначення характеру, масштабів та наслідків інциденту [12].

На етапі реакції на інцидент приймаються термінові заходи для нейтралізації загрози та запобігання подальшому поширенню атаки. Це може включати блокування вторгнення, відключення компрометованих систем або впровадження інших заходів безпеки.

Після нейтралізації загрози необхідно відновити нормальне функціонування інформаційних систем та відновити доступність та цілісність

даних. Цей етап також включає аналіз причин інциденту та розробку заходів для попередження подібних інцидентів у майбутньому.

Останній етап реагування полягає в оцінці ефективності заходів, прийнятих під час реагування на інцидент, а також вдосконаленні процесів та стратегій реагування для забезпечення більш ефективної відповіді на подібні загрози у майбутньому.

Під час реагування на інциденти інформаційної безпеки керуються декількома ключовими принципами, які допомагають забезпечити ефективність та адекватність дій персоналу. Вони зображені на рис. 1.7.

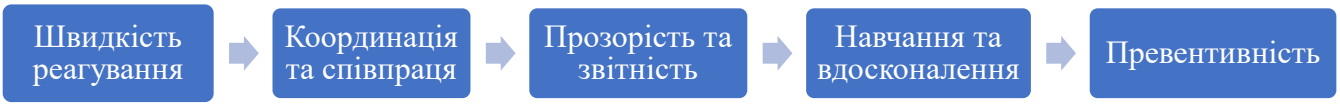


Рис. 1.7. Принципи реагування на інциденти

Швидке реагування на інциденти дозволяє мінімізувати збитки та обмежити поширення атаки. Чим швидше виявлено, нейтралізовано та відновлено інформаційні ресурси, тим менше можливостей для зловмисників завдати шкоди [13].

Швидкість реагування на інциденти інформаційної безпеки є критичним елементом у забезпеченні безпеки та стійкості сучасних організацій у цифровому середовищі. Цей аспект стає все більш важливим у світлі постійно зростаючих загроз кібербезпеки та високо спеціалізованих атак, які можуть швидко призвести до серйозних наслідків для бізнесу та репутації.

Швидке реагування базується на ряді ключових принципів та практичних стратегій. Перш за все, важливо мати налагоджені механізми виявлення інцидентів, такі як системи виявлення вторгнень, аналіз журналів подій та моніторинг мережевого трафіку. Ці механізми дозволяють оперативно виявляти аномальні активності та підозрілі патерни, що можуть свідчити про потенційні загрози.

Далі, важливо мати встановлені процедури та протоколи реагування на інциденти, які дозволяють оперативно та ефективно реагувати на виявлені загрози. Ці процедури повинні включати в себе розподіл обов'язків та відповідальності серед персоналу, забезпечення необхідних ресурсів для реагування та чітку послідовність дій у кризових ситуаціях.

Крім того, важливо мати налагоджені комунікаційні канали та механізми сповіщення, які дозволяють оперативно координувати реагування на інциденти та забезпечувати швидку передачу інформації між відповідальними особами. Це дозволяє уникнути затримок у прийнятті рішень та оперативно реагувати на змінні обставини.

Швидкість реагування на інциденти інформаційної безпеки є ключовим чинником у мінімізації збитків та обмеженні впливу кіберзагроз на бізнес. Організації, які розуміють важливість швидкого реагування та мають налагоджені механізми та процедури для цього, знаходяться в кращому становищі для захисту своїх інформаційних ресурсів та забезпечення безпеки своїх даних.

Ефективне реагування на інциденти потребує тісної співпраці між різними відділами та підрозділами організації, включаючи IT, безпеку, правовий відділ та вище керівництво [14].

Координація та співпраця визначаються як ключові складові в процесі реагування на кіберінциденти. У світлі постійно зростаючих загроз кібербезпеки, здатність організацій швидко та ефективно співпрацювати між різними відділами та підрозділами стає критично важливою для успішного подолання інцидентів та мінімізації їх наслідків.

Співпраця включає в себе взаємодію різних зацікавлених сторін у процесі реагування на інциденти, включаючи вище керівництво, IT-персонал, безпеку інформації, правові відділи та інші відділи організації. Завдяки спільним зусиллям та взаємодії між цими відділами можна швидко та ефективно виявляти, аналізувати та реагувати на загрози.

Ключовою складовою співпраці є координація дій між відділами та підрозділами. Це включає в себе розподіл обов'язків та відповідальності, визначення ролей та функцій кожного відділу у процесі реагування, а також забезпечення чіткої послідовності дій. Наприклад, IT-відділ може бути відповідальним за технічні аспекти реагування, в той час як відділ безпеки інформації може бути відповідальним за аналіз потенційних загроз та розробку стратегій захисту.

Крім того, важливо мати налагоджені комунікаційні канали та механізми сповіщення, які дозволяють оперативно обмінюватися інформацією між відділами та підрозділами. Це дозволяє уникнути затримок у прийнятті рішень та забезпечує швидку передачу інформації про виявлені загрози та аномальні активності [15].

Однією з ключових переваг співпраці та координації є можливість обмінюватися досвідом та знаннями між відділами та підрозділами. Це дозволяє організації вдосконалювати свої процеси реагування на інциденти та підвищувати свій рівень підготовленості до потенційних загроз.

У світі постійно зростаючих кіберзагроз, співпраця та координація стають ключовими елементами успішного реагування на інциденти інформаційної безпеки. Організації, які розуміють важливість цих аспектів та мають налагоджені механізми для їх реалізації, знаходяться в кращому становищі для захисту своїх інформаційних ресурсів та забезпечення стійкості своїх систем у цифровому середовищі.

Під час реагування на інциденти важливо забезпечити прозорість та звітність щодо виявлених загроз, заходів, які були прийняті, та їхніх наслідків.

Прозорість та звітність становлять невід'ємну складову успішного реагування на інциденти інформаційної безпеки. Ці принципи визначаються не лише як етичні принципи, а й як стратегічні елементи, що сприяють вдосконаленню та забезпеченню стійкості систем безпеки.

Прозорість вимагає, щоб всі зацікавлені сторони мали доступ до достовірної, зрозумілої та вичерпної інформації щодо інциденту. Це означає, що

організації повинні відкрито ділитися інформацією про те, що сталося, як вони відреагували, і які наслідки могли бути. Прозорість допомагає забезпечити довіру як серед власників, так і серед клієнтів та інших зацікавлених сторін.

Звітність означає не лише представлення інформації, але й відповідальність за дії та рішення. Організації повинні представляти повні та достовірні звіти про інциденти, їхні наслідки та прийняті заходи. Звітність вимагає визначення відповідальних осіб, вказання чітких термінів та стандартів, які дотримуються під час реагування на інцидент.

Прозорість та звітність важливі з кількох причин. По-перше, вони сприяють побудові довіри. Коли організація є прозорою та звітною щодо своїх дій у разі інциденту, це створює віру в її здатність ефективно управляти ризиками та вирішувати проблеми [16].

По-друге, прозорість та звітність сприяють навчанню та вдосконаленню. Аналіз інцидентів та відкритий звіт про них дозволяють організаціям зрозуміти свої слабкі місця, навчитися на їхніх помилках та запобігти подібним проблемам у майбутньому. Цей процес навчання стає ключовим фактором у підвищенні рівня безпеки та ефективності управління ризиками.

Проте, для досягнення ефективної прозорості та звітності, необхідно мати відповідні механізми збору, аналізу та комунікації інформації. Крім того, організації повинні мати чітко визначені політики та процедури, які регулюють звітність та відповідальність під час реагування на інциденти.

Прозорість та звітність в реагуванні на інциденти інформаційної безпеки не лише сприяють побудові довіри та навчанню, але й є ключовими елементами системного управління ризиками та забезпечення стійкості організації. Їхнє використання дозволяє організаціям ефективно реагувати на інциденти та підвищує загальний рівень безпеки та захищеності.

Реагування на інциденти є важливою частиною процесу вдосконалення системи безпеки. Інциденти слід розглядати як можливість для навчання та покращення стратегій та процедур безпеки.

Навчання та вдосконалення в управлінні інцидентами інформаційної безпеки є необхідними складовими для сучасних організацій, які стикаються зі зростаючими загрозами кібербезпеки. Швидкі та складні зміни в технологіях та методах атак вимагають постійного навчання та вдосконалення для забезпечення ефективного реагування на інциденти. У цьому есе розглянемо ключові стратегії та практичні аспекти навчання та вдосконалення в управлінні інцидентами інформаційної безпеки.

Навчання та вдосконалення в управлінні інцидентами інформаційної безпеки є критично важливими аспектами для забезпечення стійкості та надійності інформаційних систем. Шляхом постійного оновлення знань, тренувань персоналу та вдосконалення процедур інцидентного реагування організації можуть підвищити свою готовність до реагування на найскладніші кіберзагрози та мінімізувати можливі збитки.

Крім реагування на поточні інциденти, важливо приділяти увагу і превентивним заходам, спрямованим на попередження майбутніх загроз та атак.

Превентивність у контексті управління інцидентами інформаційної безпеки є однією з найважливіших складових стратегії захисту. Цей підхід передбачає прийняття передбачуваних та проактивних заходів для запобігання виникненню потенційних загроз інформаційній безпеці перед тим, як вони можуть спричинити реальний збиток. Він включає в себе ряд стратегій, методів та практик, спрямованих на попередження атак, виявлення вразливостей та зниження ризику для систем безпеки.

Однією з основних складових превентивної стратегії є проведення системного аналізу і оцінки потенційних загроз та ризиків інформаційній безпеці. Це включає в себе ідентифікацію потенційних загроз, визначення їхніх потенційних наслідків та оцінку ймовірності їх виникнення. На основі цих даних можуть бути розроблені стратегії та заходи для мінімізації ризиків та підвищення рівня захисту.

Ще одним важливим аспектом превентивної стратегії є регулярне проведення аудитів та перевірок безпеки, що дозволяють виявляти потенційні

вразливості та слабкі місця в інформаційних системах перед тим, як вони можуть бути використані зловмисниками. Ці аудити можуть включати в себе технічні аналізи і сканування, а також перевірку внутрішніх процедур та політик безпеки [17].

Превентивна стратегія також передбачає впровадження заходів з освіти та навчання персоналу з питань кібербезпеки. Навчання співробітників щодо потенційних загроз, методів захисту та процедур реагування на інциденти допомагає знизити ризик внутрішніх загроз та збільшити рівень обізнаності з питань безпеки.

Нарешті, превентивна стратегія включає в себе постійне вдосконалення систем безпеки на основі зібраної інформації та аналізу попередніх інцидентів. Регулярне оновлення програмного забезпечення, вдосконалення політик безпеки та впровадження новітніх технологій допомагає підвищити ефективність захисту та знизити ймовірність виникнення інцидентів у майбутньому.

Превентивна стратегія в управлінні інцидентами інформаційної безпеки є ключовим елементом для забезпечення стійкості та безпеки інформаційних систем. Шляхом передбачування та запобігання потенційним загрозам заздалегідь можна знизити ризики та забезпечити ефективний захист даних інформаційних систем.

Ці принципи допомагають організувати ефективну та системну стратегію реагування на інциденти, що є ключовим аспектом забезпечення безпеки та стійкості інформаційних систем. Виконання цих принципів дозволяє організаціям не лише ефективно вирішувати поточні проблеми, але й підвищувати рівень підготовленості та реагування на майбутні загрози.

## Висновки до розділу 1

Сутність та класифікація інцидентів інформаційної безпеки визначаються як сукупність подій або ситуацій, що можуть спричинити або вже спричинили

порушення безпеки інформації чи систем. Ці інциденти можуть бути класифіковані за різними критеріями, такими як тип атаки, метод їх виконання, або наслідки для інформаційних ресурсів. Це допомагає розуміти різноманітність загроз та розробляти відповідні стратегії захисту.

Методи та процедури виявлення інцидентів включають в себе різноманітні техніки та інструменти, призначені для виявлення аномальних або підозрілих активностей у мережах та системах. Це можуть бути системи виявлення вторгнень, аналіз журналів подій, моніторинг мережевого трафіку та інші методи, які допомагають вчасно виявляти потенційні загрози та реагувати на них.

Основні етапи та принципи реагування на інциденти визначають послідовність дій, що необхідні для ефективного вирішення ситуації. Це включає виявлення і аналіз інциденту, реакцію на нього, відновлення та відновлення нормального функціонування, а також оцінку та вдосконалення процесів для майбутнього запобігання подібним інцидентам.

Управління інцидентами інформаційної безпеки є складним та багатогранним процесом, який вимагає розуміння сутності та класифікації інцидентів, ефективних методів виявлення та процедур реагування. Впровадження цих аспектів у практику дозволяє організаціям забезпечувати ефективний захист інформаційних ресурсів та знижувати ризик виникнення інцидентів у цифровому середовищі.

# Розділ 2 ПРАКТИЧНИЙ ДОСВІД РЕАГУВАННЯ НА ІНЦИДЕНТИ

У сучасних умовах стрімкої цифровізації та зростання кіберзагроз, ефективне реагування на інциденти інформаційної безпеки є критичним компонентом захисту організаційних ресурсів. Аналізуючи реальні випадки інцидентів, можна виявити основні вразливості та розробити відповідні стратегії для їх усунення. Це дозволяє організаціям підвищити свою стійкість до кіберзагроз та забезпечити безперервність бізнес-процесів.

## 2.1 Огляд реальних випадків інцидентів інформаційної безпеки.

Сучасні організації в умовах зростаючої цифровізації постійно стикають з різноманітними загрозами та вразливостями. Аналізуючи конкретні приклади кібератак на великі компанії та урядові установи, можна глибше зрозуміти природу цих загроз, їхні наслідки та важливість впровадження ефективних заходів інформаційної та кібербезпеки.

Згідно зі звітом Verizon про розслідування витоків даних за 2024 рік [18], на атаки соціальної інженерії припадає 17% усіх витоків даних і 10% інцидентів кібербезпеки, що робить соціальну інженерію одним з трьох найпоширеніших векторів кібератак. Такі атаки часто націлені на співробітників організацій з метою обманом змусити їх розкрити особисту інформацію. Якщо зловмисникам вдається зламати паролі співробітників, які захищають корпоративні ресурси, вони можуть отримати несанкціонований доступ до критично важливих даних і систем організації. Ці випадки підкреслюють важливість постійного вдосконалення заходів кібербезпеки, зокрема підвищення обізнаності співробітників про методи соціальної інженерії та впровадження більш строгих протоколів безпеки.

У січні 2023 року компанія Mailchimp, відома платформа для email-маркетингу та розсилок, виявила несанкціоноване проникнення до своєї інфраструктури. Відповідно до заяви компанії, зловмисник отримав доступ до

одного з інструментів, які Mailchimp використовує для адміністрування облікових записів користувачів та підтримки клієнтів. Попередні розслідування показали, що зловмисник скористався методами соціальної інженерії для отримання облікових даних співробітників Mailchimp. Отримавши ці дані, зловмисник зміг отримати доступ до інформації 133 акаунтів Mailchimp. Хоча компанія стверджує, що конфіденційна інформація не була викрадена, цей злом міг призвести до витоку імен клієнтів та їхніх електронних адрес. Інцидент підкреслює важливість забезпечення кібербезпеки в організаціях, особливо в контексті захисту від соціальної інженерії та належного управління обліковими даними співробітників. Це також демонструє необхідність постійного моніторингу та удосконалення заходів безпеки для запобігання подібним інцидентам у майбутньому [19].

У травні 2022 року компанія Cisco, що спеціалізується на цифрових комунікаціях, зіткнулася з серйозним інцидентом інформаційної безпеки, коли зловмисник проник у її внутрішню мережу. В ході внутрішнього розслідування з'ясувалося, що зловмисник використав складні голосові фішингові атаки для отримання доступу до облікового запису Google одного зі співробітників компанії. Через синхронізацію облікових даних у браузері, зловмисник зміг легко отримати доступ до внутрішніх систем Cisco. Після отримання початкового доступу зловмисник намагався залишатися в мережі якомога довше, прагнучи підвищити свій рівень доступу до конфіденційних ресурсів компанії. Проте команда безпеки Cisco вчасно виявила проникнення та успішно видалила зловмисника з мережі. Незважаючи на це, пізніше група зловмисників, відома як Yanluowang, оприлюднила витоки файлів, отриманих під час атаки, на своєму веб-сайті. Представники Cisco заявили, що цей інцидент не вплинув на поточну діяльність компанії [20].

У січні 2022 року Міжнародний комітет Червоного Хреста (МКЧХ) зазнав серйозної кібератаки, що призвела до масового витоку даних. Колишній радник МКЧХ з питань кібервійни Лукаш Олійник зазначив, що це, ймовірно, був найбільший і найчутливіший злом в історії МКЧХ та, можливо, усіх

гуманітарних організацій. Було скомпрометовано дані понад 515 000 людей, розлучених зі своїми сім'ями через конфлікти, міграцію та інші катастрофи. Спочатку вважалося, що витік даних стався через атаку на субпідрядника, але розслідування показало, що атака була спрямована безпосередньо на сервери МКЧХ. Зловмисники скомпрометували привілейовані облікові записи, використовували методи бічного переміщення для підвищення своїх привілеїв та діяли під виглядом адміністраторів, щоб отримати доступ до конфіденційних даних [21].

У вересні 2023 року дослідники штучного інтелекту Microsoft випадково виклали 38 терабайт приватних даних під час публікації навчальних даних з відкритим кодом на GitHub. Витік включав конфіденційну корпоративну інформацію з робочих станцій двох співробітників, серед яких були секрети, приватні ключі, паролі та понад 30 000 внутрішніх повідомлень Microsoft Teams. Причиною інциденту стала неправильна конфігурація токенів SAS від Azure, що надало доступ до всього облікового запису сховища замість конкретних файлів. Цей випадок підкреслює важливість правильного налаштування доступу до хмарних сервісів та належного захисту конфіденційної інформації [22].

У травні 2022 року компанія Apple подала до суду на стартап Rivos, що займається розробкою мікросхем, за звинуваченням у крадіжці комерційної таємниці. Причиною позову стало те, що Rivos звільнив понад 40 колишніх працівників Apple, і принаймні двоє з них забрали з собою гігабайти конфіденційної інформації перед тим, як приєднатися до стартапу. Apple припускає, що Rivos найняв колишніх співробітників для роботи над конкуруючою технологією "система на чіпі" (SoC), на розробку якої Apple витратила мільярди доларів і понад десять років досліджень. Доступ до комерційної таємниці, пов'язаної з SoC, суттєво допоміг би Rivos у конкурентній боротьбі з Apple [23].

У лютому 2022 року старший науковий співробітник Yahoo Цянь Санг викрав інтелектуальну власність компанії через 45 хвилин після отримання пропозиції про роботу від The Trade Desk. Yahoo виявила, що Санг завантажив

570 000 файлів зі службового ноутбука на особисті зовнішні накопичувачі. Викрадені дані включали вихідний код AdLearn, технології Yahoo для оптимізації реклами на основі машинного навчання, а також інші файли з репозиторіїв Yahoo на Github [24].

Атака на ланцюжок поставок SolarWinds у 2020 році була однією з найскладніших кіберінцидентів свого часу, націленою на компанію SolarWinds, провідного постачальника програмного забезпечення для управління мережею. Хакери скомпрометували процес розробки програмного забезпечення SolarWinds, інтегрувавши шкідливий бекдор у оновлення їхньої платформи Orion. Згодом ці скомпрометовані оновлення були розповсюджені серед клієнтів, включаючи численні урядові установи США. Це дозволило зловмисникам отримати несанкціонований доступ до чутливих систем, викрадаючи дані та порушуючи безпеку критичних інфраструктур. Цей інцидент підкреслює важливість забезпечення безпеки ланцюжків постачання програмного забезпечення та потребу у постійних вдосконаленнях у кібербезпеці для запобігання подібним атакам [25].

У травні 2023 року компанія Progress Software виявила вразливість нульового дня у своєму програмному забезпеченні для передачі файлів MOVEit Transfer. Ця вразливість дозволила зловмисникам отримати доступ до серверів MOVEit і викрасти дані клієнтів. Згодом кілька хакерських груп, зокрема банда вимагачів Cl0p, використали цю вразливість, націлившись на численні організації, включаючи урядові установи, медичні заклади та компанії, такі як British Airways, Boots і BBC. До вересня кібератака зачепила понад 2000 організацій, викривши дані 60 мільйонів людей. Цей злам вважається однією з найбільших і найшкідливіших кібератак в історії через кількість постраждалих осіб, фінансові збитки та довготривалі наслідки [26].

Проведені атаки по рокам зображені в табл. 2.1.

Таблиця 2.1

Випадки інцидентів інформаційної безпеки

| № | Рік | Компанія | На що спрямована атака |
|---|---|---|---|
| 1 | 2020 | Solarwinds | Атака на ланцюжок поставок, зокрема процес розробки програмного забезпечення solarwinds, інтеграція шкідливого бекдору в оновлення платформи Orion. |
| 2 | 2022 | Cisco | Серйозний інцидент інформаційної безпеки, зловмисник проник у внутрішню мережу через голосові фішингові атаки, отримав доступ до облікового запису Google одного зі співробітників. |
| 3 | | Міжнародний комітет Червоного Хреста | Масовий витік даних, скомпрометовано дані понад 515 000 людей, зловмисники використали методи бічного переміщення для підвищення привілеїв. |
| 4 | | Apple | Крадіжка комерційної таємниці, стартап Rivos звільнив понад 40 колишніх працівників Apple, які забрали з собою конфіденційну інформацію. |
| 5 | | Yahoo | Старший науковий співробітник викрав інтелектуальну власність компанії, завантажив 570 000 файлів зі службового ноутбука на особисті зовнішні накопичувачі. |
| 6 | 2023 | Mailchimp | Несанкціоноване проникнення до інфраструктури, зловмисник скористався методами соціальної інженерії для отримання облікових даних співробітників. |
| 7 | | Microsoft | Витік 38 терабайт приватних даних під час публікації навчальних даних з відкритим кодом на github, неправильна конфігурація токенів SAS від Azure. |
| 8 | | Progress Software | Вразливість нульового дня у програмному забезпеченні для передачі файлів moveit Transfer, зловмисники викрали дані клієнтів, зокрема банда вимагачів Cl0p. |

Огляд реальних випадків інцидентів інформаційної безпеки демонструє масштаб і серйозність сучасних кіберзагроз. Випадки, такі як атака на SolarWinds та інциденти з участю Mailchimp і Cisco, підкреслюють необхідність постійного вдосконалення заходів захисту, впровадження комплексних стратегій кібербезпеки та підвищення обізнаності співробітників. Ці інциденти також свідчать про важливість міжнародного співробітництва і стандартизації у сфері кібербезпеки. Використовуючи отримані уроки, організації можуть краще підготуватися до майбутніх викликів і забезпечити надійний захист своїх інформаційних систем.

## 2.2 Аналіз ефективності використання процедур реагування на інциденти в практиці.

Для оцінки ефективності процесу реагування на інциденти CREST [27] розробила модель оцінки ефективності кожного з шести етапів реагування. Процес реагування на інциденти, відповідно до цього ппроцесу, поділяється на шість етапів: підготовка, ідентифікація, стримування, ліквідація, відновлення та аналіз уроків.

Основні етапи оцінки ефективності включають аналіз елементів під час симуляцій інцидентів, підготовка набору інструментів для реагування, моніторинг систем на предмет ознак компрометації, реалізацію стратегій стримування, видалення причини інциденту, відновлення систем та проведення постінцидентного аналізу. Вони зображені на рис. 2.1. Незважаючи на неможливість повної підготовки до майбутніх інцидентів, важливо розробити здатність до виявлення проблем на ранніх стадіях і визначити ключових учасників з відповідними процедурами комунікації. Ефективний план реагування на інциденти повинен бути формально визначений і періодично оцінюватись для збереження його ефективності.


Рис. 2.1. Основні етапи оцінки ефективності

Під час підготовки до оцінки реагування на інцидент (IR) дуже важливо забезпечити ефективність різних ключових засобів контролю. Це передбачає ретельний аналіз під час періодичних, полегшених імітаційних тестових сценаріїв інциденту. Ці тестування повинні охоплювати кілька важливих елементів, включаючи шаблон плану реагування на інцидент і контактні дані основних зацікавлених сторін. До таких зацікавлених сторін належать внутрішні та зовнішні спеціалісти, технічні спеціалісти, постачальники, юридичний відділ, відділ кадрів, відділ зв'язків з громадськістю, керівництво компанії та зовнішні регуляторні органи [28].

Крім того, необхідно оцінити наявність і готовність ресурсів для аналізу інцидентів. Ці ресурси включають списки портів, аналізатори пакетів, аналізатори протоколів та необхідну документацію, таку як системи виявлення вторгнень (IDS), системи управління інформацією та подіями безпеки (SIEM), мережеві схеми та інвентаризацію активів. Забезпечення легкодоступності та

актуальності цих інструментів і документів є життєво важливим для швидкого та ефективного реагування на інциденти.

Крім того, підготовка набору інструментів для реагування на інциденти є ключовим компонентом готовності до IR. Цей набір повинен охоплювати засоби судової візуалізації, необхідні для ретельного аналізу та збереження цифрових доказів. Він також повинен включати фізичні інструменти, такі як викрутки, кусачки, ліхтарі, рукавички та камери, які можуть знадобитися під час розслідування на місці події. Наявність цих інструментів гарантує, що фахівці, які здійснюють реагування, будуть оснащені для ефективного вирішення широкого спектру сценаріїв інцидентів.

Під час аудиту важливо шукати задокументовані докази того, що така підготовка та ресурси наявні. Ця документація слугує доказом прихильності організації до підтримання надійної спроможності реагування на інциденти. Ретельно оцінивши ці елементи, організації можуть підвищити свою готовність і забезпечити більш ефективне та дієве реагування на потенційні інциденти безпеки. Такий комплексний підхід не лише зменшує ризики, але й демонструє дотримання найкращих практик в управлінні реагуванням на інциденти [29].

Для ефективного виявлення потенційних інцидентів безпеки важливо забезпечити наявність комплексних систем і механізмів моніторингу для виявлення різних індикаторів компрометації (IOC). До таких індикаторів належить незвичний вихідний мережевий трафік, що може свідчити про витік даних або зв'язок з командно-контрольними серверами. Крім того, створення нових адміністративних користувачів є важливим тривожним сигналом, що потенційно вказує на несанкціонований доступ або підвищення привілеїв.

Моніторинг також має охоплювати аномалії в активності облікових записів привілейованих користувачів, наприклад, перший вхід в систему, що може свідчити про скомпрометовані облікові записи. Географічні аномалії, такі як нестандартні спроби входу в систему з неочікуваних місць, також важливо відстежувати, оскільки вони можуть свідчити про несанкціонований доступ з іноземних або підозрілих регіонів. Збільшення кількості зчитувань бази даних,

що потенційно може свідчити про дамп бази даних, є ще одним важливим індикатором, який слід ретельно відстежувати.

Крім того, раптове збільшення кількості запитів до одного і того ж файлу може свідчити про спроби використання вразливостей або збору конфіденційної інформації. Підозрілі зміни записів у реєстрі або системних файлах, які можуть бути частиною дій шкідливого програмного забезпечення, також потребують пильного моніторингу. Несподівані виправлення, які не відповідають регулярному графіку оновлень, можуть свідчити про те, що зловмисник намагається замести сліди або впровадити шкідливі виправлення.

Зрештою, слід ретельно відстежувати ознаки розподіленої активності, що характеризується надмірним трафіком, спрямованим на порушення доступності сервісів – DDoS. Переконавшись, що системи та інструменти моніторингу налаштовані на виявлення цих індикаторів, організації можуть значно підвищити свою здатність виявляти інциденти безпеки та оперативно реагувати на них. Такий проактивний підхід до моніторингу та виявлення є фундаментальним компонентом надійної системи кібербезпеки, що дозволяє організаціям зменшити ризики та ефективно реагувати на потенційні загрози [30].

Для ефективного стримування інцидентів безпеки необхідно переглянути та забезпечити наявність комплексних стратегій стримування, що охоплюють низку критично важливих дій. По-перше, важливо визначити план дій, заснований на потенційному впливі інцидентів. Ця стратегія повинна передбачати чіткі, практичні кроки, які можна швидко реалізувати для зменшення шкоди.

Блокування несанкціонованого доступу є першочерговим заходом стримування, який повинен включати як запобігання, так і реєстрацію таких спроб. Це гарантує, що несанкціонований доступ буде не лише зупинено, але й зафіксовано для подальшого аналізу. Так само важливим є блокування джерел шкідливого програмного забезпечення, таких як шкідливі адреси електронної пошти, IP-адреси та веб-сайти. Ці дії запобігають поширенню шкідливого програмного забезпечення та зменшують ризик подальшого зараження.

Закриття певних портів і поштових серверів, які визначені як вектори для атаки, може значно зменшити поверхню атаки. Крім того, впровадження фільтрації брандмауера для контролю трафіку і запобігання несанкціонованим з'єднанням є важливим заходом для обмеження поширення інциденту.

У деяких випадках переміщення домашніх сторінок веб-сайтів може бути необхідним кроком для збереження цілісності сайту при одночасному вирішенні основних проблем. Ізоляція уражених систем у мережі допомагає локалізувати загрозу та запобігти її поширенню на інші частини інфраструктури [31].

Регулярне та систематичне резервне копіювання є ще одним важливим компонентом стратегії стримування. Резервні копії гарантують, що дані можуть бути відновлені в разі компрометації, мінімізуючи час простою і втрату даних. В екстремальних випадках може знадобитися вимкнення систем, щоб запобігти подальшому пошкодженню та провести ретельне розслідування і усунення наслідків.

Для забезпечення ефективності етапу ліквідації інциденту дуже важливо впровадити та оцінити кілька ключових засобів контролю. Основною метою цього етапу є усунення першопричини інциденту, що часто збігається із заходами з локалізації. Мета полягає не лише в усуненні безпосередньої загрози, але й в усуненні першопричини та самого інциденту, таким чином викорінюючи компрометацію.

Перевірка усунення загрози має важливе значення для підтвердження того, що загроза була повністю усунута. Цього можна досягти шляхом моніторингу мережевого трафіку та перегляду критичних журналів для виявлення будь-яких залишкових ознак інциденту. Постійний моніторинг допомагає переконатися, що зусилля з усунення загрози є успішними і що в мережі не залишилося ніяких загроз [32].

Кроки з ліквідації повинні включати кілька конкретних дій. До них належить усунення атаки з мережі, що передбачає ідентифікацію та ізоляцію уражених систем, а також усунення шкідливої присутності. Видалення шкідливого програмного забезпечення із заражених систем є ще одним

важливим кроком, який гарантує, що не залишиться жодних слідів шкідливого коду. Вимкнення порушених облікових записів користувачів запобігає подальшому несанкціонованому доступу та допомагає захистити скомпрометовані облікові записи.

Виявлення та усунення вразливостей, які були використані під час інциденту, має вирішальне значення. Це передбачає розуміння того, як зловмисники отримали доступ, і вжиття заходів для усунення цих слабких місць, щоб запобігти майбутнім інцидентам. Ретельна оцінка вразливостей і план їх усунення повинні бути частиною процесу ліквідації [33].

Належне поводження з доказами під час інциденту також є ключовим елементом контролю. Повинен існувати офіційний процес збереження та обробки доказів для забезпечення їхньої прийнятності в судовому процесі та дотримання відповідних законів. Цей процес повинен включати кроки з документування та захисту доказів, підтримуючи чіткий ланцюжок їх зберігання.

Процеси роботи з доказами мають бути розроблені таким чином, щоб зібрані докази були прийнятними в суді та відповідали всім відповідним вимогам законодавства. Це включає належне документування, безпечне зберігання та чіткі процедури збору та обробки цифрових доказів.

Щоб забезпечити ефективність етапу відновлення при реагуванні на інцидент, необхідно оцінити і перевірити кілька ключових засобів контролю. Комплексний план відновлення повинен включати такі основні завдання, як визначення пріоритетності відновлення системи, відновлення даних з резервних копій, оновлення та інформування зацікавлених сторін, усунення подібних вразливостей у мережі та заповнення детального звіту про інцидент. Ці завдання є важливими для структурованого та ефективного процесу відновлення.

Визначення пріоритетності відновлення системи передбачає виявлення критично важливих систем і забезпечення їх відновлення в першу чергу, щоб мінімізувати операційні збої. Відновлення даних з резервних копій слід проводити ретельно, щоб забезпечити цілісність і безперервність даних. Не менш

важливо інформувати зацікавлені сторони протягом усього процесу відновлення, повідомляючи їх про прогрес і будь-який потенційний вплив на їхню діяльність.

Усунення подібних вразливостей у мережі є проактивним заходом для запобігання майбутнім інцидентам. Це передбачає проведення ретельного огляду мережі для виявлення та усунення будь-яких слабких місць, які можуть бути використані. Заповнення звіту про інцидент має вирішальне значення для документування інциденту, вжитих заходів та отриманих уроків, які можуть бути використані в майбутньому для реагування на інциденти.

План відновлення повинен також охоплювати основні методи відновлення, включаючи відновлення заражених систем з відомих чистих джерел. Це слід робити з урахуванням пріоритетів, щоб гарантувати, що критичні функції будуть відновлені в першу чергу. Повторне підключення мереж і відновлення, відтворення або виправлення інформації є важливими кроками для повернення до нормальної роботи. Документування змін, внесених до інфраструктури під час процесу відновлення, є важливим для збереження точних та актуальних записів про конфігурацію та стан системи [34].

Також необхідно враховувати роботу з частинами систем або мереж, які не підлягають відновленню. Це передбачає наявність планів на випадок непередбачених ситуацій для систем, які можуть бути непоправно пошкоджені або скомпрометовані.

Підтвердження того, що системи працюють нормально після відновлення, має вирішальне значення. Цього можна досягти, провівши незалежні тести на проникнення в уражені системи та здійснивши оцінку засобів контролю безпеки. Ці кроки гарантують, що системи захищені та функціонують належним чином.

Після відновлення систем і тестування засобів контролю важливо надати зацікавленим сторонам короткий звіт про те, що відбулося. Цей звіт має бути наданий протягом одного дня після події, щоб зацікавлені сторони були поінформовані та заспокоєні. Чітке і своєчасне інформування є ключем до збереження довіри і прозорості протягом усього процесу реагування на інцидент.

Для забезпечення надійної стратегії реагування на інциденти (IR) важливо проводити ретельний аналіз після інцидентів та інтегрувати отримані уроки в поточну практику безпеки. Цей процес включає кілька ключових завдань, які необхідно проаналізувати та перевірити.

Комплексний аналіз після інциденту повинен включати глибокий аналіз процесу управління інцидентами. Цей аналіз повинен оцінити, наскільки швидко були вжиті заходи для виявлення інциденту, реагування на нього та відновлення після нього. Він також повинен визначити, як довго зловмисники були присутні в системі до її виявлення, які дії вони вчинили або планували вчинити, а також рівень захисту критично важливих систем і конфіденційної інформації під час інциденту. Оцінка роботи персоналу та керівництва з ліквідації інциденту має вирішальне значення, так само як і забезпечення належного документування всіх ключових обговорень та рішень, прийнятих під час заходу з ліквідації інциденту. Під час аналізу слід також вивчити ефективність впроваджених процедур і визначити будь-які кроки або дії, які могли перешкоджати зусиллям з відновлення [35].

Виявлення уроків, отриманих з інцидентів безпеки, є ще одним важливим завданням. Ці уроки повинні бути офіційно задокументовані та доведені до відома відповідних зацікавлених сторін, щоб забезпечити їх широке розуміння та впровадження. Документація повинна призвести до реальних дій, які можна застосувати для покращення реагування на інциденти в майбутньому. Крім того, обмін ключовими питаннями та найкращими практиками в усіх сферах бізнесу, а не лише в командах IT та кібербезпеки, є життєво важливим для комплексного вдосконалення.

Після інциденту безпеки вкрай важливо оновити плани та процедури IP. Це включає в себе перегляд методологій або процесів управління інцидентами безпеки, щоб відобразити нові знання, отримані в результаті інциденту. План реагування на інциденти безпеки слід оновити, включивши до нього будь-які нові стратегії та тактики, які довели свою ефективність. На основі отриманих уроків слід вдосконалити засоби управлінського контролю, такі як програми

навчання та підвищення обізнаності. Технічні засоби контролю, включаючи виправлення, налаштування системних журналів і використання інструментів запобігання/виявлення вторгнень, також слід переглянути і оновити, щоб усунути будь-які прогалини або слабкі місця, виявлені в результаті інциденту. Нарешті, слід чітко визначити та оновити ролі та обов'язки щодо реагування на інциденти, щоб гарантувати, що кожен розуміє свої обов'язки у разі виникнення інциденту в майбутньому.

Отже, хоча неможливо повністю підготуватися до невідомих майбутніх інцидентів, певні елементи процесу реагування на інциденти вимагають ретельної підготовки, щоб забезпечити ефективну мінімізацію наслідків інциденту.

Одним з найважливіших елементів є розробка надійних засобів виявлення інцидентів. Раннє виявлення проблем має вирішальне значення для запобігання переростанню незначних проблем у серйозні інциденти. Як показано в нашому тематичному дослідженні, обмежені можливості виявлення призвели до того, що проблему було помічено лише тоді, коли було порушено роботу поштових служб. Покращення цих можливостей може забезпечити швидке виявлення та вирішення проблем, мінімізуючи їхній вплив.

Іншим важливим елементом є визначення ключових зацікавлених сторін і встановлення чітких процедур комунікації. Ефективне прийняття рішень під час інциденту залежить від здатності інформувати всі зацікавлені сторони, зберігаючи при цьому конфіденційність інформації, пов'язаної з інцидентом. Проведення симуляційних навчань з реагування на інцидент є безцінним інструментом для виявлення прогалин у процесі реагування та підвищення готовності всіх зацікавлених сторін [36].

Зрештою, план реагування на інциденти повинен бути не тільки формально визначений, але й періодично оцінюватися для забезпечення його постійної ефективності. Регулярні оцінки допомагають адаптувати план до нових загроз і вразливостей, гарантуючи, що він залишається актуальним і надійним. Впровадження чітко визначеної та зрілої системи реагування на інциденти, такої

як та, що розроблена CREST, охоплює всі критичні аспекти оцінки реагування на інциденти. Такий комплексний підхід гарантує, що організації будуть краще підготовлені до реагування на інциденти, пом'якшення їх наслідків і швидкого відновлення, тим самим підтримуючи цілісність і безперервність своїх операцій.

### 2.3 Вивчення найкращих практик та висновки з практичного досвіду

Ефективне реагування на інциденти має важливе значення для зменшення цих ризиків і забезпечення швидкого відновлення. У цьому розділі розглядаються найкращі практики реагування на кіберінциденти, підкреслюється необхідність комплексних політик, чітких комунікаційних протоколів та чітко визначених ролей у командах реагування на інциденти.

Створення політики та плану реагування на інциденти має фундаментальне значення. Це передбачає визначення подій, які кваліфікуються як інциденти, та створення організаційної структури з чітким розподілом ролей та обов'язків для реагування на ці події. План має охоплювати всі системи, включно з тими, якими керують зовнішні постачальники, забезпечуючи цілісний підхід до управління інцидентами. Маючи визначену структуру, посадові особи виборчих органів можуть швидко та ефективно реагувати на кіберінциденти, мінімізуючи потенційну шкоду та підтримуючи операційну цілісність.

Розробка процедур реагування на інциденти та звітування про них є ще однією важливою практикою. Детальні процедури повинні охоплювати всі етапи обробки інцидентів, як зазначено в контрольному переліку NIST SP 800-61 «Обробка інцидентів». Це забезпечує структуроване і систематичне реагування на інциденти, від початкового виявлення до локалізації, ліквідації та відновлення. Комплексні процедури допомагають підтримувати послідовність і ретельність в управлінні інцидентами, що дозволяє ефективно зменшити загрози і відновити нормальну роботу [37].

Встановлення правил комунікації із зовнішніми сторонами під час інцидентів має важливе значення для забезпечення прозорості та координації.

Чітко розроблений план комунікацій визначає, про які інциденти необхідно повідомляти зовнішнім суб'єктам, таким як ЗМІ, правоохоронні та регуляторні органи, а також відповідні терміни та відповідальних членів команди. Це сприяє своєчасному і точному поширенню інформації, допомагає керувати громадською думкою і дотриманням законодавства, зберігаючи при цьому конфіденційні деталі.

Вибір відповідної структури команди та кадрової моделі є життєво важливим для готовності до реагування на інциденти. Організації повинні вирішити, чи створювати внутрішню групу реагування на інциденти, чи передавати ці функції на аутсорсинг, враховуючи такі фактори, як необхідний досвід, потенційний стрес і витрати на управління інцидентами, а також необхідність цілодобової доступності. Добре структурована команда гарантує, що інцидентами займаються кваліфіковані фахівці, здатні ефективно реагувати на різні технічні та нетехнічні виклики.

Налагодження взаємовідносин і ліній зв'язку між командою реагування на інциденти та іншими внутрішніми і зовнішніми групами покращує співпрацю під час інцидентів. Ефективні відносини та чіткі канали зв'язку з юридичним відділом, правоохоронними органами та іншими зацікавленими сторонами мають вирішальне значення для скоординованого реагування на інциденти. Це гарантує, що всі необхідні сторони залучені та поінформовані, що сприяє єдиному підходу до управління інцидентами та відновлення.

Визначення послуг, що надаються групою реагування на інцидент, також має важливе значення. Чіткий розподіл ролей та обов'язків гарантує, що кожен член команди розуміє свої конкретні завдання та внесок, що призводить до більш ефективного та результативного реагування на інциденти. Чітко визначені послуги допомагають впорядкувати процеси обробки інцидентів і гарантують, що всі критичні питання будуть вирішені оперативно [38].

Кадрове забезпечення та навчання команди реагування на інциденти є ключовими для підтримки готовності. Постійне навчання гарантує, що члени команди добре обізнані з новітніми процедурами та технологіями реагування на

інциденти і можуть плавно переходити від реагування до відновлення. Регулярні тренування та навчання підвищують здатність команди реагувати на реальні інциденти, забезпечуючи високий рівень готовності та компетентності.

Таблиця 2.3.

Вивчення найкращих практик та висновки з практичного досвіду

| № | **Практика** | **Опис** |
|---|---|---|
| 1 | Створення політики та плану реагування на інциденти | Визначення подій, які кваліфікуються як інциденти, та створення організаційної структури з чітким розподілом ролей та обов'язків. |
| 2 | Розробка процедур реагування на інциденти та звітування про них | Детальні процедури, що охоплюють всі етапи обробки інцидентів від початкового виявлення до відновлення. |
| 3 | Встановлення правил комунікації із зовнішніми сторонами | Чіткий план комунікацій для повідомлення зовнішнім суб'єктам, таким як ЗМІ, правоохоронні та регуляторні органи. |
| 4 | Вибір відповідної структури команди та кадрової моделі | Вирішення, чи створювати внутрішню групу реагування, чи передавати ці функції на аутсорсинг. |
| 5 | Налагодження взаємовідносин та ліній зв'язку | Покращення співпраці під час інцидентів через чіткі канали зв'язку з юридичним відділом, правоохоронними органами та іншими зацікавленими сторонами. |
| 6 | Визначення послуг, що надаються групою реагування на інцидент | Чіткий розподіл ролей та обов'язків для кожного члена команди, що гарантує ефективне реагування на інциденти. |
|  | Кадрове забезпечення та навчання команди реагування на інциденти | Постійне навчання та тренування членів команди для підтримки високого рівня готовності та компетентності. |

На закінчення, хоча повна готовність до всіх потенційних майбутніх інцидентів недосяжна, створення надійної системи реагування на інциденти має вирішальне значення. Необхідно розвивати можливості виявлення, щоб забезпечити ранню ідентифікацію проблем до їх ескалації. Повинні бути впроваджені ефективні процедури комунікації для забезпечення своєчасного і конфіденційного обміну інформацією між зацікавленими сторонами. Регулярне моделювання реагування на інциденти є безцінним для виявлення та усунення прогалин у процесі реагування. План реагування на інциденти повинен бути не тільки формально визначений, але й періодично оцінюватися для забезпечення його ефективності. Прийняття чітко визначеної та зрілої системи реагування на

інциденти, подібної до тієї, що розроблена CREST, забезпечує всебічне охоплення всіх критичних аспектів управління інцидентами, підвищуючи загальну стійкість та безпеку.

**Висновок до розділу 2**

Аналіз реальних випадків інцидентів інформаційної безпеки, представлених у розділі, демонструє, що кіберзагрози є складними та постійно еволюціонують. Зокрема, випадки з компаніями Mailchimp, Cisco, Microsoft, Apple, Yahoo, SolarWinds, та Progress Software виявляють різноманітні методи атак, включаючи соціальну інженерію, фішингові атаки, компрометацію ланцюжка постачання, і викрадення інтелектуальної власності. Ці інциденти підкреслюють важливість постійного вдосконалення заходів кібербезпеки, впровадження комплексних стратегій захисту та підвищення обізнаності співробітників про методи соціальної інженерії.

Також важливим є розвиток ефективних процедур реагування на інциденти, які включають підготовку, ідентифікацію, стримування, ліквідацію, відновлення та аналіз уроків. Ефективність цих процедур може бути оцінена за допомогою моделі, розробленої CREST, яка включає аналіз елементів під час симуляцій інцидентів, підготовку набору інструментів для реагування, моніторинг систем на предмет ознак компрометації, реалізацію стратегій стримування та видалення причин інциденту. Важливим аспектом є наявність задокументованих доказів підготовки та готовності до інцидентів.

Крім того, досягнення кіберстійкості вимагає інтеграції нових технологій, таких як штучний інтелект, для прогнозування потенційних збоїв та моделювання наслідків різних сценаріїв. Не менш важливим є врахування змін клімату та їх впливу на безпеку, а також підвищення стійкості ланцюгів постачання.

На основі отриманих уроків, організації можуть вдосконалювати свої плани реагування на інциденти, забезпечуючи швидке виявлення, ефективну

комунікацію та оперативне відновлення після інцидентів. Таким чином, комплексний підхід до управління інформаційною безпекою сприяє зменшенню ризиків і забезпеченню надійного захисту критично важливих даних і систем.

# Розділ 3 РЕКОМЕНДАЦІЇ ЩОДО ПОКРАЩЕННЯ ОРГАНІЗАЦІЇ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 3.1 Розробка стратегій покращення процедур реагування на інциденти

У сучасних умовах стрімкого розвитку інформаційних технологій та постійного зростання кіберзагроз ефективне реагування на інциденти інформаційної безпеки стає ключовим аспектом забезпечення стійкості організацій. Впровадження новітніх технологій, систематичне навчання персоналу та розробка стратегій (рис. 3.1) покращення процедур реагування на інциденти є критично важливими для зниження ризиків і забезпечення захисту критично важливих інформаційних активів.


Рис. 3.1. Схема послідовності розробки стратегій

Аналіз існуючих політик реагування на інциденти є важливим кроком у реагуванні на інциденти інформаційної безпеки, оскільки він гарантує, що наявні протоколи є комплексними та ефективними. Цей етап передбачає ретельне вивчення поточної системи реагування на інциденти з метою виявлення сильних і слабких сторін, а також областей, які потребують вдосконалення. Аналіз слід починати з ретельного вивчення задокументованих політик і процедур, щоб переконатися, що вони відповідають найкращим галузевим практикам і регуляторним вимогам. Ключові аспекти, які слід розглянути, включають сферу застосування політик, чіткість розподілу ролей та обов'язків, а також визначені процедури виявлення, локалізації, усунення та відновлення інцидентів.

Оцінка обсягу політики реагування на інциденти має важливе значення для визначення того, чи охоплює вона всі потенційні типи інцидентів безпеки, включаючи кібератаки, витоки даних та системні збої. Політика повинна чітко визначати критерії ідентифікації інцидентів, деталізуючи конкретні індикатори компрометації, які запускають процес реагування. Крім того, мають бути чітко визначені ролі та обов'язки команди реагування на інциденти, щоб кожен член команди розумів свої обов'язки та субординацію під час інциденту [39].

Процедурні аспекти політики реагування на інциденти повинні бути ретельно вивчені, щоб переконатися, що вони передбачають детальні та практичні кроки для кожного етапу управління інцидентом. Це включає початкове виявлення та аналіз інциденту, стратегії стримування для запобігання подальшої шкоди, заходи з ліквідації для усунення загрози, а також процеси відновлення для відновлення нормальної роботи. Кожен крок повинен бути задокументований з чіткими інструкціями, щоб сприяти скоординованому та ефективному реагуванню.

Крім того, необхідно оцінити ефективність комунікаційних протоколів в рамках політики реагування на інциденти. Необхідно розробити чіткі інструкції для внутрішніх і зовнішніх комунікацій, включаючи повідомлення зацікавленим сторонам, регуляторним органам і потенційно постраждалим сторонам. Це гарантує, що вся відповідна інформація буде поширюватися швидко і точно, підтримуючи прозорість і відповідність вимогам протягом усього процесу реагування на інцидент.

Інтеграція сучасних інструментів реагування на інциденти є ключовим етапом у підвищенні спроможності організації ефективно управляти інцидентами інформаційної безпеки. Оскільки кіберзагрози продовжують ускладнюватися і ставати дедалі частішими, використання передових технологічних рішень стає необхідним для забезпечення своєчасного виявлення, аналізу, локалізації та усунення цих загроз. Сучасні інструменти реагування на інциденти охоплюють широкий спектр технологій, включаючи системи управління інформацією та подіями безпеки (SIEM), рішення для виявлення та

реагування на кінцевих точках (EDR) і передові платформи для розвідки загроз, кожна з яких відіграє важливу роль у життєвому циклі реагування на інциденти.

Впровадження систем SIEM дозволяє агрегувати та співвідносити дані про події безпеки з різних джерел, забезпечуючи централізоване бачення ландшафту безпеки. Ці системи використовують складні алгоритми і методи машинного навчання для виявлення патернів, що вказують на зловмисну активність, що дозволяє швидше і точніше виявляти інциденти безпеки. Можливості моніторингу в режимі реального часу систем SIEM сприяють швидкому виявленню потенційних загроз, значно скорочуючи вікно вразливості та обмежуючи потенційний вплив на активи організації [40].

Інструменти виявлення та реагування на кінцеві точки підвищують видимість і контроль над кінцевими точками, які часто є основними цілями кібератак. Рішення EDR постійно контролюють діяльність кінцевих точок, виявляючи підозрілу поведінку на ранніх стадіях атаки та реагуючи на неї. Інтегруючи інструменти EDR, організації можуть швидко ізолювати скомпрометовані кінцеві точки, проводити криміналістичний аналіз, щоб зрозуміти масштаб і характер загрози, а також ініціювати відповідні заходи з локалізації та усунення наслідків. Такий проактивний підхід зводить до мінімуму ризик латерального руху в мережі і гарантує нейтралізацію загроз до того, як вони зможуть ескалуватися.

Передові платформи розвідки загроз надають важливу контекстну інформацію про нові загрози і вразливості. Інтегруючи розвідку загроз у процес реагування на інциденти, організації можуть випереджати потенційних супротивників, використовуючи актуальну інформацію для розробки стратегій захисту. Ці платформи полегшують обмін даними про загрози між представниками спільноти безпеки, сприяючи спільним зусиллям у сфері оборони та посилюючи загальний стан безпеки [41].

Симуляційне навчання персоналу є важливим етапом реагування на інциденти інформаційної безпеки, що підвищує готовність та ефективність команди реагування на інциденти в організації. Цей метод навчання передбачає

створення реалістичних сценаріїв, які імітують потенційні інциденти безпеки, що дозволяє членам команди відпрацьовувати свої стратегії реагування в контрольованому середовищі. Основна мета симуляційних тренінгів - забезпечити, щоб персонал добре знав свої ролі та обов'язки, що дозволить їм швидко та ефективно реагувати на реальні інциденти.

Імітаційні вправи забезпечують динамічну платформу для перевірки ефективності планів і процедур реагування на інциденти. Відтворюючи різні сценарії загроз, такі як витік даних, атаки з вимогою викупу або атаки на відмову в обслуговуванні, організації можуть оцінити свою готовність і виявити будь-які слабкі місця в своїх стратегіях реагування. Такі вправи допомагають вдосконалити процеси виявлення та аналізу, гарантуючи, що співробітники служби безпеки зможуть швидко розпізнати та оцінити характер і масштаби інциденту.

Крім того, симуляційні тренування покращують процес прийняття рішень і координацію між членами команди. Воно сприяє створенню середовища співпраці, де учасники можуть практикувати протоколи комунікації як всередині команди, так і з зовнішніми зацікавленими сторонами, такими як регуляторні та правоохоронні органи. Ефективна комунікація є життєво важливою під час інциденту, оскільки вона забезпечує швидке поширення точної інформації, що дозволяє скоординоване реагування та мінімізує плутанину.

Ще однією значною перевагою симуляційних тренувань є можливість оцінити інтеграцію та функціональність інструментів і технологій реагування на інциденти. За допомогою цих вправ організації можуть перевірити розгортання та ефективність своїх систем управління інформацією та подіями безпеки (SIEM), рішень для виявлення та реагування на кінцеві точки (EDR) та інших критично важливих інструментів. Виявлення будь-яких технічних проблем або прогалин під час симуляцій дозволяє своєчасно виправити та оптимізувати ці інструменти, забезпечуючи їх безперебійну роботу під час реальних інцидентів [42].

Крім того, симуляційне навчання дає цінну інформацію про людський фактор реагування на інциденти. Воно підкреслює сильні сторони та сфери для покращення індивідуальної та командної роботи, спрямовуючи зусилля на цілеспрямоване навчання та професійний розвиток. Регулярне проведення симуляційних тренувань допомагає підтримувати високий рівень готовності, оскільки вони залучають персонал служби безпеки та інформують його про новітні загрози та методи реагування.

Регулярний перегляд та оновлення стратегій реагування на інциденти є важливими компонентами підтримки стійкості організації до нових загроз інформаційної безпеки. Цей безперервний процес гарантує, що система реагування на інциденти залишається ефективною, актуальною та узгодженою з останніми практиками безпеки та ландшафтами загроз. Регулярні огляди передбачають систематичне вивчення існуючих стратегій з метою виявлення будь-яких прогалин, неефективності або сфер, що потребують вдосконалення.

Під час процесу перегляду дуже важливо оцінити ефективність поточних політик і процедур за допомогою метрик і показників ефективності, отриманих на основі минулих інцидентів. Така оцінка допомагає зрозуміти сильні та слабкі сторони поточних можливостей реагування. Посмертний аналіз інциденту та уроки, винесені з попередніх інцидентів, дають цінну інформацію про те, що спрацювало добре, а що ні, і дозволяють внести необхідні корективи до стратегій реагування.

Оновлення стратегій передбачає включення нової інформації про нові загрози та вразливості. Для цього необхідно бути в курсі останніх розвідувальних даних про загрози, рекомендацій з безпеки та технологічних досягнень. Інтегруючи оновлені моделі та сценарії загроз у плани реагування, організації можуть гарантувати, що вони готові протистояти найсучаснішим і найскладнішим атакам. Крім того, технологічний прогрес в інструментах і практиках безпеки повинен бути відображений в оновлених стратегіях для покращення можливостей виявлення, аналізу та реагування [43].

Ще одним важливим аспектом оновлення стратегій реагування на інциденти є вдосконалення комунікаційних протоколів. Забезпечення чіткості, ефективності та відпрацьованості каналів і процедур зв'язку є життєво важливим для ефективної координації під час інциденту. Регулярні тренінги та симуляційні вправи допомагають тестувати і вдосконалювати ці протоколи, гарантуючи, що всі зацікавлені сторони усвідомлюють свої ролі та обов'язки.

Крім того, регуляторні та комплаєнс-вимоги часто змінюються, що вимагає періодичних оновлень для забезпечення відповідності стратегій реагування на інциденти найновішим правовим та галузевим стандартам. Це передбачає перегляд політик і процедур для включення будь-яких нових регуляторних зобов'язань або керівних принципів.

## 3.2 Впровадження нових технологій та інструментів для ефективного виявлення та аналізу інцидентів

Впровадження нових технологій та інструментів для ефективного виявлення та аналізу інцидентів є ключовим елементом забезпечення кібербезпеки в сучасних організаціях. Схема цього процесу зображена на рис. 3.2.


Рис. 3.2 Схема впровадження нових технологій

Першочерговим завданням є оцінка поточних можливостей, що передбачає детальний аналіз існуючих інструментів та технологій, які використовуються для виявлення та аналізу інцидентів. Це дозволяє виявити прогалини та визначити сфери, що потребують вдосконалення. Такий аналіз є фундаментальним етапом, оскільки він забезпечує об'єктивне розуміння поточного стану системи кібербезпеки організації та визначає базис для подальших дій.

Наступним кроком є визначення вимог до нових інструментів і технологій. Це включає формулювання конкретних цілей і задач, які повинні бути досягнуті з їхньою допомогою, враховуючи унікальні потреби організації та поточний ландшафт загроз. Важливо враховувати специфіку діяльності організації, її інформаційні потоки, критичні ресурси та потенційні вразливості. Визначення вимог дозволяє не тільки чітко окреслити критерії вибору нових рішень, але й забезпечити їхню відповідність стратегічним цілям організації.

Третій етап полягає в дослідженні ринку та виборі постачальника. Це вимагає ретельного аналізу доступних на ринку інструментів і технологій, їхньої

функціональності, сумісності з існуючими системами, масштабованості та вартості. Особливу увагу слід приділити репутації постачальників, їхній здатності надавати підтримку та оновлення продуктів, а також відгукам інших користувачів. Проведення такого дослідження дозволяє зробити обґрунтований вибір на користь тих рішень, які найбільше відповідають потребам організації та забезпечують максимальну ефективність у виявленні та аналізі інцидентів [44].

Підтвердження концепції (Proof of Concept, PoC) є критичним етапом впровадження нових технологій для ефективного виявлення та аналізу інцидентів. Під час цього етапу необхідно здійснити перевірку концепції, щоб протестувати інструменти з короткого списку в контрольованому середовищі. Це дозволяє оцінити їхню ефективність, можливості інтеграції та зручність для користувача. Тестування в реальних умовах дає змогу визначити, наскільки вибрані інструменти відповідають очікуванням і вимогам організації, та ідентифікувати потенційні проблеми, які можуть виникнути під час їхнього впровадження.

Залучення зацікавлених сторін є наступним важливим кроком. Необхідно залучити ключові зацікавлені сторони з IT, безпеки та керівництва для збору відгуків та забезпечення відповідності цілям організації. Їхня участь і підтримка є критичними для успішного впровадження нових технологій, оскільки це дозволяє забезпечити гармонійне інтегрування нових рішень у існуючі процеси та структури, а також врахувати всі вимоги та побажання різних відділів.

Після позитивного завершення PoC, можна переходити до етапу закупівель та ліцензування. Це включає завершення процесу закупівель, укладання контрактів та отримання необхідних ліцензій на обрані інструменти та технології. Важливо забезпечити прозорість і чіткість у договірних зобов'язаннях, а також передбачити можливості для подальшої підтримки та оновлення придбаних рішень.

Не менш важливим етапом є планування інтеграції та впровадження. Для цього необхідно розробити детальний план, що включає терміни виконання робіт, розподіл ресурсів та стратегії управління ризиками. План має бути

всебічним і враховувати всі аспекти впровадження, від технічних вимог до навчання персоналу. Ефективне планування інтеграції забезпечує мінімізацію простоїв та збоїв у роботі організації, що дозволяє швидко досягти бажаних результатів і підвищити рівень кібербезпеки.

Етап встановлення та конфігурації передбачає інсталяцію та налаштування нових інструментів і технологій з забезпеченням їх належної інтеграції з існуючими системами та процесами. Цей процес включає налаштування параметрів, що відповідають специфічним вимогам організації, та забезпечення безперебійної роботи нових рішень у загальній IT-інфраструктурі [45].

На завершальному етапі проводиться ретельне тестування та валідація нових інструментів і технологій. Це необхідно для перевірки їхньої ефективності у виявленні та аналізі інцидентів. У разі виявлення недоліків або неефективності, конфігурації коригуються на основі результатів тестування, що дозволяє досягти максимальної ефективності та надійності впроваджених рішень.

### 3.3 Заходи щодо підвищення кваліфікації персоналу та підготовки до реагування на інциденти.

Роль працівників у реагуванні на інциденти має вирішальне значення для підтримання надійної системи безпеки. Кожен працівник повинен усвідомлювати свої обов'язки щодо виявлення та повідомлення про інциденти безпеки. Це передбачає всебічне розуміння того, що є інцидентом безпеки, включаючи такі загрози, як фішингові електронні листи, підозрілі веб-сайти та будь-які інші аномальні дії, які можуть поставити під загрозу безпеку організації. Співробітники повинні володіти знаннями, щоб оперативно повідомляти про такі інциденти через відповідні канали.

Реагування на інциденти - це колективна відповідальність, яка виходить за межі IT-відділу. Це вимагає скоординованих зусиль, коли кожен працівник, незалежно від його посадових обов'язків, навчений розпізнавати та реагувати на потенційні загрози безпеці. Це стосується не лише IT-спеціалістів, але й

працівників рецепції, які можуть зіткнутися з підозрілими телефонними дзвінками чи відвідувачами, а також працівників відділу кадрів, які можуть отримати шахрайські електронні листи з вимогою надати конфіденційну інформацію про співробітників [46]. Забезпечивши належну підготовку всіх співробітників та усвідомлення ними своїх ролей у реагуванні на інциденти, організації можуть створити пильний та оперативний персонал, здатний ефективно зменшувати ризики безпеки. Безперервне навчання та програми підвищення обізнаності мають важливе значення для зміцнення цієї культури безпеки та забезпечення того, щоб працівники залишалися пильними та проактивними у захисті організації від нових загроз. Заходи підготовки до реагування на інциденти зображені на рис. 3.3.

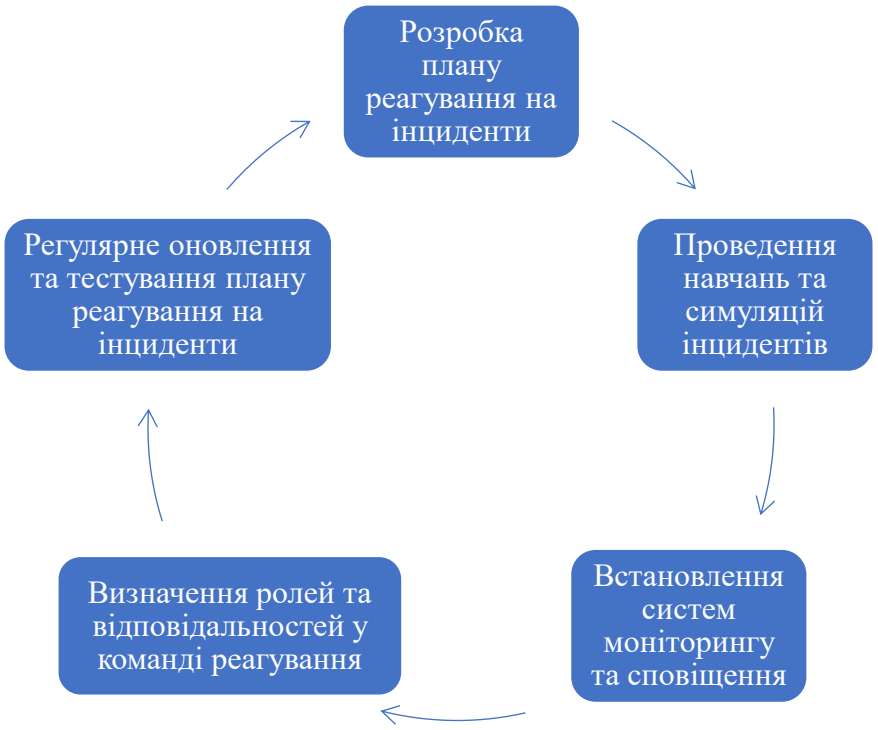


Рис. 3.3. Заходи підготовки до реагування на інциденти

Ефективне навчання з реагування на інциденти підвищує професійну майстерність співробітників, підвищуючи їхню впевненість і компетентність у роботі з інцидентами безпеки. Це сприяє розвитку культури безпеки в організації, гарантуючи, що кожен працівник розуміє важливість своєї ролі в підтримці кібербезпеки. Це навчання також відкриває можливості для

професійного розвитку та кар'єрного зростання, оскільки працівники набувають цінних навичок і знань, які мають вирішальне значення в сучасному цифровому ландшафті.

Безперервне та всебічне навчання з реагування на інциденти має важливе значення для вирішення проблем, пов'язаних з мінливим характером кіберзагроз. Регулярні оновлення та курси підвищення кваліфікації гарантують, що працівники будуть в курсі останніх загроз та вразливостей, тим самим підвищуючи їхню здатність ефективно реагувати на них. Пристосування навчання до конкретних потреб організації з урахуванням таких факторів, як галузь, розмір і складність бізнесу, ще більше підвищує його ефективність.

Крім того, таке навчання сприяє розробці цілісної та скоординованої стратегії реагування на інциденти. Воно готує співробітників до злагодженої роботи під час інциденту безпеки, забезпечуючи ефективну комунікацію та співпрацю між різними відділами. Такий комплексний підхід не лише зміцнює загальну систему безпеки організації, але й сприяє підвищенню стійкості та адаптивності персоналу.

Насамкінець, навчання з реагування на інциденти є життєво важливим елементом надійної стратегії кібербезпеки. Надаючи працівникам знання та навички виявлення та повідомлення про інциденти безпеки, компанії можуть значно знизити ризик кібератак, убезпечити свою діяльність, захистити репутацію та фінансову стабільність. Інвестиції в навчання в кінцевому підсумку сприяють створенню безпечного та стійкого організаційного середовища.

Для покращення навичок персоналу та підготовки до реагування на інциденти вкрай важливими є регулярні тренінги та симуляції. Ці заходи гарантують, що співробітники залишатимуться вправними у розпізнаванні новітніх загроз та інцидентів і реагуванні на них. Таке навчання має бути комплексним і охоплювати різноманітні потенційні сценарії, щоб створити надійний потенціал реагування. Чіткі комунікаційні протоколи є не менш важливими, оскільки вони сприяють ефективному управлінню інцидентами, забезпечуючи своєчасне і точне поширення інформації серед усіх зацікавлених

сторін. Це допомагає координувати зусилля з реагування та пом'якшувати наслідки інцидентів безпеки [47].

Надання доступу до передових інструментів і технологій є ще одним важливим заходом. Ці ресурси підвищують здатність персоналу виявляти, аналізувати і швидко та ефективно реагувати на загрози. Передові технології, такі як сучасні системи виявлення загроз та автоматизовані інструменти реагування, можуть значно підвищити ефективність та результативність процесів реагування на інциденти.

Розвиток культури безперервного навчання в організації ще більше посилює готовність до реагування на інциденти. Заохочення працівників до отримання сертифікатів з кібербезпеки та участі в програмах професійного розвитку дозволяє підтримувати їхні знання та навички в актуальному стані. Таке прагнення до безперервного навчання гарантує, що команда залишається добре підготовленою до протидії новим кіберзагрозам.

Ці комплексні заходи - регулярні тренінги та симуляції, чіткі комунікаційні протоколи, доступ до передових інструментів і технологій та культура безперервного навчання - разом підвищують стійкість організації та її здатність реагувати на кіберінциденти. Інвестуючи в ці сфери, організації можуть створити більш дієздатну та проактивну команду реагування на інциденти, краще оснащену для захисту критично важливих активів та підтримки операційної цілісності перед обличчям кіберзагроз.

## Висновок до розділу 3

У розділі було висвітлено рекомендації щодо покращення організації реагування на інциденти інформаційної безпеки, що включають розробку стратегій, впровадження нових технологій та підвищення кваліфікації персоналу. Аналіз існуючих політик реагування на інциденти є важливим кроком для гарантування їхньої ефективності та відповідності найкращим галузевим практикам. Оцінка поточних можливостей дозволяє виявити прогалини та

визначити сфери, що потребують вдосконалення. Визначення вимог та цілей нових інструментів і технологій забезпечує їхню відповідність специфічним потребам організації та поточному ландшафту загроз. Проведення ретельного дослідження ринку та вибір постачальника на основі таких критеріїв, як функціональність, сумісність, масштабованість та вартість, дозволяє зробити обґрунтований вибір на користь найбільш ефективних рішень.

Інтеграція сучасних інструментів реагування на інциденти, таких як системи управління інформацією та подіями безпеки (SIEM) і рішення для виявлення та реагування на кінцевих точках (EDR), значно підвищує спроможність організації ефективно управляти інцидентами. Такі інструменти забезпечують швидке та точне виявлення загроз, їх аналіз та нейтралізацію, що знижує ризик латерального руху в мережі та мінімізує вплив інцидентів на організацію. Передові платформи розвідки загроз надають важливу контекстну інформацію про нові загрози та вразливості, полегшуючи розробку стратегій захисту.

Симуляційне навчання персоналу сприяє підвищенню готовності та ефективності команди реагування на інциденти. Воно забезпечує всебічне розуміння ролей і обов'язків, покращує процес прийняття рішень та координацію між членами команди, а також дозволяє оцінити інтеграцію та функціональність інструментів і технологій реагування на інциденти. Регулярне проведення таких тренувань допомагає підтримувати високий рівень готовності, залучаючи персонал служби безпеки та інформуючи його про новітні загрози та методи реагування.

Таким чином, комплексний підхід до управління інформаційною безпекою, який включає постійне вдосконалення стратегій, впровадження сучасних технологій та систематичне навчання персоналу, є необхідною умовою для забезпечення стійкості організації перед сучасними кіберзагрозами.

# ВИСНОВКИ

У контексті сучасного стрімкого розвитку інформаційних технологій та зростання кіберзагроз, ефективне управління інцидентами інформаційної безпеки стає невід'ємною частиною стратегії захисту будь-якої організації. У розділах, присвячених теоретичним аспектам реагування на інциденти, класифікації загроз, методам виявлення та реагування, а також вдосконаленню процедур безпеки, були висвітлені ключові моменти, що сприяють забезпеченню інформаційної безпеки на високому рівні.

По-перше, було підкреслено значення розробки науково обґрунтованих підходів до управління інцидентами. Це включає створення теоретичних моделей, методів та алгоритмів для виявлення, аналізу та відновлення після інцидентів. Такий підхід забезпечує можливість своєчасного виявлення загроз, їх ефективного нейтралізування та мінімізації потенційних втрат. Інциденти інформаційної безпеки можуть мати різні форми і використовувати численні техніки для уникнення виявлення, тому важливо застосовувати комплексні методи моніторингу та аналізу.

По-друге, виявлення та ідентифікація інцидентів є критично важливими етапами, оскільки від їхньої ефективності залежить здатність організації своєчасно реагувати на загрози. Використання систем виявлення вторгнень (IDS), аналіз лог-файлів та застосування методів машинного навчання дозволяють виявляти аномальні дії та ідентифікувати загрози, які не можуть бути виявлені традиційними методами. Це забезпечує основу для подальших заходів щодо реагування та відновлення.

Класифікація інцидентів, аналіз їхніх характеристик, джерел та потенційних наслідків дозволяє розробити оптимальні стратегії реагування. Розуміння характеру загрози, джерела та способу її реалізації сприяє вибору правильних методів нейтралізації та запобігання подібним інцидентам у майбутньому. Класифікація також допомагає систематизувати загрози і визначити пріоритети для вжиття заходів з реагування.

Процедури реагування на інциденти включають в себе низку заходів, спрямованих на нейтралізацію загрози, мінімізацію збитків та відновлення нормального функціонування систем. Швидке та ефективне реагування дозволяє зменшити вплив інциденту на бізнес-процеси, що підвищує стійкість організації до кіберзагроз. Крім того, важливою складовою є міждисциплінарний підхід та інтеграція знань з різних галузей, таких як комп'ютерні науки, криптографія, менеджмент та правознавство.

Регулярне проведення симуляційного навчання персоналу та впровадження новітніх технологій, таких як системи управління інформацією та подіями безпеки (SIEM) та рішення для виявлення та реагування на кінцевих точках (EDR), значно підвищує готовність організації до реагування на інциденти. Використання штучного інтелекту та машинного навчання для аналізу поведінки користувачів та системних компонентів допомагає виявляти загрози, що не можуть бути ідентифіковані традиційними методами.

Крім того, прозорість та звітність щодо виявлених загроз і прийнятих заходів є ключовими елементами успішного реагування на інциденти. Вони сприяють побудові довіри, навчанню та вдосконаленню процесів управління інцидентами. Важливо мати налагоджені комунікаційні канали та механізми сповіщення, які дозволяють оперативно координувати дії між різними відділами та підрозділами організації.

На завершення, ефективне управління інцидентами інформаційної безпеки включає комплексний підхід, що поєднує теоретичні знання, сучасні технології та систематичне навчання персоналу. Це дозволяє організаціям своєчасно реагувати на загрози, мінімізувати збитки та забезпечувати безперервність бізнес-процесів у умовах постійно зростаючих кіберзагроз.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions / Ö. Aslan et al. *Electronics*. 2023. Vol. 12, no. 6. P. 1333. URL: https://doi.org/10.3390/electronics12061333

2. Safitra M. F., Lubis M., Fakhrurroja H. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*. 2023. Vol. 15, no. 18. P. 13369. URL: https://doi.org/10.3390/su151813369

3. Kure H., Islam S., Razzaque M. An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences*. 2018. Vol. 8, no. 6. P. 898. URL: https://doi.org/10.3390/app8060898

4. Kaur R., Gabrijelčič D., Klobučar T. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. *Information Fusion*. 2023. P. 101804. URL: https://doi.org/10.1016/j.inffus.2023.101804

5. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review / U. Tariq et al. *Sensors*. 2023. Vol. 23, no. 8. P. 4117. URL: https://doi.org/10.3390/s23084117

6. Exploring manet security aspects: analysis of attacks and node misbehaviour issues / B. U. I. Khan et al. *Malaysian Journal of Computer Science*. 2022. Vol. 35, no. 4. P. 307–338. URL: https://doi.org/10.22452/mjcs.vol35no4.2

7. A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanisms and Challenges / T. Sasi et al. *Journal of Information and Intelligence*. 2023. URL: https://doi.org/10.1016/j.jiixd.2023.12.001

8. A system for generating and injecting indistinguishable network decoys / B. M. Bowen et al. *Journal of Computer Security*. 2012. Vol. 20, no. 2-3. P. 199–221. URL: https://doi.org/10.3233/jcs-2011-0439

9. Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions / A. Giannaros et al. *Journal of Cybersecurity and Privacy*. 2023. Vol. 3, no. 3. P. 493–543. URL: https://doi.org/10.3390/jcp3030025

10. Kilincer I. F., Ertam F., Sengur A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*. 2021. Vol. 188. P. 107840. URL: https://doi.org/10.1016/j.comnet.2021.107840

11. Alkasassbeh M., Al-Haj Baddar S. Intrusion Detection Systems: A State-of-the-Art Taxonomy and Survey. *Arabian Journal for Science and Engineering*. 2022. URL: https://doi.org/10.1007/s13369-022-07412-1

12. Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity / P. Dini et al. *Applied Sciences*. 2023. Vol. 13, no. 13. P. 7507. URL: https://doi.org/10.3390/app13137507

13. Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction / N. Ahmed et al. *Sensors*. 2022. Vol. 22, no. 20. P. 7896. URL: https://doi.org/10.3390/s22207896

14. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience / S. Saeed et al. *Sensors*. 2023. Vol. 23, no. 16. P. 7273. URL: https://doi.org/10.3390/s23167273

15. Defining organisational information security culture–Perspectives from academia and industry / A. da Veiga et al. *Computers & Security*. 2020. Vol. 92. P. 101713. URL: https://doi.org/10.1016/j.cose.2020.101713

16. A systematic analysis of failures in protecting personal health data: A scoping review / J. Pool et al. *International Journal of Information Management*. 2024. Vol. 74. P. 102719. URL: https://doi.org/10.1016/j.ijinfomgt.2023.102719

17. Shamsan Saleh A. M. Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. Blockchain: *Research and Applications*. 2024. P. 100193. URL: https://doi.org/10.1016/j.bcra.2024.100193

18. 2024 Data Breach Investigations Report. *Verzion*. URL: https://www.verizon.com/business/resources/reports/dbir/

19. Information About a Recent Mailchimp Security Incident. *Mailchimp*. URL: https://mailchimp.com/newsroom/january-2023-security-incident/

20. Cisco Event Response: Corporate Network Security Incident. *Cisco.* URL: https://sec.cloudapps.cisco.com/security/center/resources/corp_network_security_incident

21. Cyber attack on ICRC: What we know. *ICRC.* URL: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know%E2%80%8B#:~:text=Update%3A%2024%20June%202022.,in%20a%20sophisticated%20cyber%20attack.

22. 2023 Threat Intelligence Year in Review: Key Insights and Developments. *Microsoft.* URL: https://www.microsoft.com/en-us/security/security-insider/emerging-threats/2023-threat-intelligence-year-in-review-key-insights-and-development

23. Report: 2.6 billion personal records compromised by data breaches in past two years — underscoring need for end-to-end encryption. *Apple*. URL: https://www.apple.com/newsroom/2023/12/report-2-point-6-billion-records-compromised-by-data-breaches-in-past-two-years/

24. SolarWinds Orion (CVE-2020-10148). *IBM*. URL: https://www.ibm.com/docs/en/randori?topic=2022-solarwinds-orion-cve-2020-10148

25. MOVEit cyberattacks: keeping tabs on the biggest data theft of 2023. *TheVerge*. URL: https://www.theverge.com/23892245/moveit-cyberattacks-clop-ransomware-government-business

26. P. Cichonski, T. Millar, T. Grance, K. Scarfone. NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide. 2012. URL: https://www.researchgate.net/publication/329972954_NIST_Special_Publication_800-61_Revision_2_Computer_Security_Incident_Handling_Guide

27. Determining the effectiveness of an incident response plan. Study based on lessons learned from a real life incident. A whitepaper. URL: https://www.bsigroup.com/LocalFiles/zh-tw/e-news/No164/CSIR-Incident-Response-WP.pdf

28. González-Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*. 2021. Vol. 21, no. 14. P. 4759. URL: https://doi.org/10.3390/s21144759

29. Aljuhani A. Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments. *IEEE Access*. 2021. Vol. 9. P. 42236–42264. URL: https://doi.org/10.1109/access.2021.3062909

30. J. Andress. Incident Response Process. URL: https://www.sciencedirect.com/topics/computer-science/incident-response-process

31. Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents / G. M. Makrakis et al. *IEEE Access*. 2021. Vol. 9. P. 165295–165325. URL: https://doi.org/10.1109/access.2021.3133348

32. Modern computing: Vision and challenges / S. S. Gill et al. *Telematics and Informatics Reports*. 2024. P. 100116. URL: https://doi.org/10.1016/j.teler.2024.100116

33. Goni A., Jahangir M. U. F., Chowdhury R. R. A Study on Cyber security: Analyzing Current Threats, Navigating Complexities, and Implementing Prevention Strategies. *International Journal of Research and Scientific Innovation*. 2024. Vol. X, no. XII. P. 507–522. URL: https://doi.org/10.51244/ijrsi.2023.1012039

34. Cyber recovery vs. disaster recovery: What's the difference? *IBM*. URL: https://www.ibm.com/blog/cyber-recovery-vs-disaster-recovery/

35. Contingency plan examples: A step-by-step guide to help your business prepare for the unexpected. *IBM*. URL: https://www.ibm.com/blog/contingency-plan-examples/

36. L. J. Fernandes, F. S. da Gama. Contingency Planning: A literature review. *SCMCC-08 Supply Chain Management and Competitiveness*. 2008. URL: https://www.researchgate.net/publication/230807504_Contingency_planning_-_a_literature_review

37. Moderating Effects of Customer Lifetime Value and Referral Value on Customer Service of Frontline Employees for Customer and Organizational

Satisfaction: A Comparative Analysis / D. Dhameeth et al. *Journal of Marketing Management (JMM)*. 2020. Vol. 8, no. 2. URL: https://doi.org/10.15640/jmm.v8n2a6

38. Patterson C. M., Nurse J. R. C., Franqueira V. N. L. Learning from cyber security incidents: A systematic review and future research agenda. Computers & Security. 2023. P. 103309. URL: https://doi.org/10.1016/j.cose.2023.103309

39. S. C. Weiner, B. R. Kinzey, J. Dean, P. B. Davis, A. Ruiz. Incident reporting: learning from experience. 2007. URL: https://www.researchgate.net/publication/239883180_INCIDENT_REPORTING_LEARNING_FROM_EXPERIENCE

40. SIEM and threat intelligence: Stay current on trending threats. *IBM*. URL: https://www.ibm.com/blog/siem-and-threat-intelligence-stay-current-on-trending-threats/

41. Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives / N. Sun et al. *IEEE Communications Surveys & Tutorials*. 2023. P. 1. URL: https://doi.org/10.1109/comst.2023.3273282

42. Evaluation of incident management strategies and technologies using an integrated traffic/incident management simulation / K. M. A. Ozbay et al. *World Review of Intermodal Transportation Research*. 2009. Vol. 2, no. 2/3. P. 155. URL: https://doi.org/10.1504/writr.2009.023305

43. ZAMFIROIU A., SHARMA R. C. Cybersecurity Management for Incident Response. *Romanian Cyber Security Journal*. 2022. Vol. 4, no. 1. P. 69–75. URL: https://doi.org/10.54851/v4i1y202208

44. Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research / J. Steinke et al. *IEEE Security & Privacy*. 2015. Vol. 13, no. 4. P. 20–29. URL: https://doi.org/10.1109/msp.2015.71

45. Svitlychnyi V. A. Protection of personal data under martial law in Ukraine. *Law and Safety*. 2023. Vol. 90, no. 3. P. 226–236. URL: https://doi.org/10.32631/pb.2023.3.19

46. Рекомендації та перспективи впровадження досвіду іноземних держав в систему формування генезису розвитку кібертехнологій у сфері безпеки

та оборони України / O. Semenenko та ін. *Journal of Scientific Papers "Social Development and Security"*. 2023. Т. 13, № 4. С. 63–80. URL: https://doi.org/10.33445/sds.2023.13.4.6

47. Gakhov S. O. Analysis of methods for detecting events and incidents of information and cyber security by SIEM systems. *Modern information security*. 2018. No. 4. URL: https://doi.org/10.31673/2409-7292.2018.040611

48. Сійчук К.І. Організація реагування на інциденти інформаційної безпеки. : матеріали Всеукр. наук.-практ. конф. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу . Київ : ДУІКТ, 28 лютого 2024. С. . URL: https://duikt.edu.ua/uploads/p_2661_62255520.pdf

49. Якименко Ю.М., Легомінова С.В., Щавінський Ю.В., Рабчун Д.І. Управління інцидентами інформаційної безпеки. Сучасні методи і засоби: навчальний посібник. Київ: Державний університет телекомунікацій, 2023. – 241с.