МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ЗАБЕЗПЕЧЕННЯ ГОТОВНОСТІ ОРГАНІЗАЦІЇ ДО РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПЛАНУВАННЯ, НАВЧАННЯ ТА ТЕСТУВАННЯ”

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

_____ Нікіта АРТЕМЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42
Нікіта АРТЕМЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Володимир ШУЛЬГА
д.і.н., старший дослідник Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____ Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Артеменку Нікіті Юрійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи забезпечення готовності організації до реагування на інциденти інформаційної безпеки: планування, навчання та тестування”, керівник кваліфікаційної роботи ШУЛЬГА Володимир, д.і.н., старший дослідник
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційні ресурси організації, що потребують захисту від загроз та ризиків, методи та підходи до оцінки і мінімізації ризиків у сфері ІБ, наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.*

4. Перелік питань, які мають бути розроблені:
   4.1. Дослідження проблеми реагування на інциденти ІБ.
   4.2. Аналіз методів та засобів для планування, навчання та тестування.
   4.3. Розроблення рекомендацій щодо планування, навчання та тестування для реагування на інциденти ІБ.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз методів та засобів для планування, навчання та тестування для реагування на інциденти ІБ.	08.04.2025	
4.	Розробка методичних підходів до організації готовності до реагування на інциденти ІБ.	15.04.2025	
5.	Практична реалізація заходів із забезпечення готовності організації до реагування на інциденти інформаційної безпеки	22.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Нікіта АРТЕМЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Володимир ШУЛЬГА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Артеменко Н.Ю. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи забезпечення готовності організації до реагування на інциденти інформаційної безпеки: планування, навчання та тестування"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач АРТЕМЕНКО Нікіта у кваліфікаційній роботі дослідив комплекс актуальних питань щодо забезпечення готовності організацій до ефективного реагування на інциденти інформаційної безпеки. У практичній частині реалізовано навчальну програму з реагування в корпоративному середовищі з оцінкою її ефективності.

Робота демонструє належний рівень теоретичної підготовки та практичних навичок здобувача. АРТЕМЕНКО Нікіта проявив самостійність, відповідальність та вміння застосовувати здобуті знання. Результати дослідження апробовані на конференції.

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

Керівник кваліфікаційної роботи _____ Володимир ШУЛЬГА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Артеменко Н.Ю. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти АРТЕМЕНКА Нікіти
на тему “Методи забезпечення готовності організації до реагування на інциденти інформаційної безпеки: планування, навчання та тестування”

Актуальність.

Актуальність обраної теми визначається зростанням кількості та складності кіберзагроз, що суттєво впливають на ефективність діяльності підприємств та організацій. В умовах швидкого розвитку цифрових технологій та посилення вимог до безперервності бізнес-процесів, здатність оперативно реагувати на інциденти інформаційної безпеки стає ключовим фактором збереження стабільності та конкурентоспроможності організацій. Тому дослідження, спрямоване на розроблення ефективних методів планування, навчання та тестування реагування на кіберінциденти, є своєчасним та практично важливим.

Позитивні сторони.

1. У роботі проаналізовано сучасні методи та засоби, що використовуються для планування та організації реагування на інциденти інформаційної безпеки, зокрема міжнародні стандарти ISO/IEC 27001, NIST і COBIT.

2. Розроблено методику проведення навчання персоналу та тестування процедур реагування, що дозволяє значно підвищити готовність організації до протидії кіберзагрозам.

3. Автор провів практичну реалізацію запропонованих методичних підходів у реальному корпоративному середовищі, що дозволило отримати практичні рекомендації для підвищення кіберстійкості організацій.

Недоліки.

1. Доцільним було б доповнити дослідження порівняльним аналізом ефективності різних програмних платформ автоматизації реагування на інциденти (SOAR-систем), а також розглянути економічні аспекти впровадження запропонованих заходів.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент:
_____ _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню підходів до формування готовності організації до реагування на інциденти інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 9 рисунків, висновків і списку використаних джерел із 64 найменувань. Загальний обсяг роботи становить 71 аркуш, з яких 7 аркушів займає список використаних джерел.

Метою роботи є підвищення рівня готовності організації до реагування на інциденти інформаційної безпеки шляхом обґрунтування та впровадження ефективних засобів планування, навчання персоналу та тестування процедур реагування.

Об'єкт дослідження – процес організації заходів із підготовки до реагування на інциденти інформаційної безпеки.

Предмет дослідження – методи та засоби забезпечення готовності організації до реагування на інциденти інформаційної безпеки.

Методи дослідження. Для реалізації поставлених завдань у роботі використано аналіз літературних джерел та нормативних документів, вивчення міжнародних стандартів (ISO/IEC 27001, NIST, COBIT) та сучасних наукових підходів до управління ризиками, методи якісного та кількісного оцінювання інцидентів, аналіз існуючих видів інцидентів, методу ТТХ (Командно-штабні навчання), методів систематизованих проведення симуляційних атак Red Team/Blue Team Exercises, емпіричні методи, методи моделювання, порівняльний аналіз.

Галузь використання. Запропоновані рішення можуть бути використані при побудові та вдосконаленні систем управління інформаційною безпекою підприємств у сфері кібербезпеки та навчанні персоналу задля покращення реагування на інциденти ІБ.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ РИЗИКАМИ, КІБЕРБЕЗПЕКА, ОЦІНКА РИЗИКІВ, РИЗИК-МЕНЕДЖМЕНТ, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРЗАГРОЗИ, СИСТЕМА МЕНЕДЖМЕНТУ, ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ПОЛІТИКА БЕЗПЕКИ.

ABSTRACT

The qualification work is devoted to the study of approaches to building an organization's readiness to respond to information security incidents. The work consists of an introduction, three chapters containing 9 figures, conclusions and a list of references of 64 titles. The total volume of the work is 71 pages, of which 7 pages are taken up by the list of references.

The purpose of the study is to increase the level of readiness of the organization to respond to information security incidents by substantiating and implementing effective means of planning, training and testing response procedures.

The object of research is the process of organizing measures to prepare for response to information security incidents.

The subject of the study are methods and means of ensuring the organization's readiness to respond to information security incidents.

Research methods. To implement the tasks set in the work, the analysis of literary sources and regulatory documents, the study of international standards (ISO/IEC 27001, NIST, COBIT) and modern scientific approaches to risk management, methods of qualitative and quantitative assessment of incidents, analysis of existing types of incidents, the TTX method (Team and Staff Exercises), methods of systematic simulation attacks Red Team/Blue Team Exercises were used; empirical methods; modeling methods; comparative analysis.

Scope of application. The proposed solutions can be used in building and improving information security management systems of enterprises in the field of cybersecurity and training personnel to improve response to security incidents.

Keywords: INFORMATION SECURITY, RISK MANAGEMENT, CYBERSECURITY, RISK ASSESSMENT, RISK MANAGEMENT, INFORMATION SECURITY, CYBER THREATS, MANAGEMENT SYSTEM, INFORMATION SECURITY INCIDENTS, SECURITY POLICY.

ЗМІСТ

ВСТУП

Актуальність теми. Інциденти інформаційної безпеки (ІБ) становлять один із найсерйозніших викликів для сучасних організацій, оскільки вони можуть не лише спричиняти значні фінансові втрати, але й мати катастрофічні наслідки для операційної діяльності, репутації та конкурентоспроможності компаній.

Втрата конфіденційної інформації, компрометація критично важливих систем, а також підрив довіри клієнтів і партнерів є лише частиною можливих негативних наслідків таких інцидентів. Зі зростанням цифрової трансформації бізнес-процесів та активним впровадженням хмарних технологій, питання оперативного реагування на кіберінциденти набуває особливої актуальності, вимагаючи від організацій підвищеної уваги до процесів управління інцидентами.

Ефективне реагування на загрози інформаційної безпеки передбачає не лише наявність передових технічних засобів захисту, а й стратегічний підхід до їхнього впровадження. Це включає розробку комплексних політик безпеки, детальне планування превентивних заходів, систематичне навчання персоналу та регулярне тестування процедур реагування, що дозволяє виявити слабкі місця та забезпечити їх усунення ще до виникнення реальних атак.

Використання міжнародних стандартів, таких як ISO/IEC 27001, NIST і COBIT, сприяє вдосконаленню процесів реагування, забезпечуючи стандартизований підхід до ідентифікації, аналізу та ліквідації загроз. Недостатня підготовка або несвоєчасне реагування може призвести до значних фінансових втрат, порушення бізнес-процесів, накладення регуляторних санкцій, а також до незворотних наслідків, зокрема повного зупинення діяльності організації.

Мета роботи – підвищення рівня готовності організації до реагування на інциденти інформаційної безпеки шляхом обґрунтування та впровадження

ефективних засобів планування, навчання персоналу та тестування процедур реагування.

Об'єкт дослідження – процес організації заходів із підготовки до реагування на інциденти інформаційної безпеки.

Предмет дослідження – методи та засоби забезпечення готовності організації до реагування на інциденти інформаційної безпеки.

Для досягнення мети у роботі поставлено такі завдання:

1. Дослідити сутність та класифікацію інцидентів інформаційної безпеки, а також нормативно-правові вимоги щодо реагування на них.

2. Проаналізувати організаційні, процедурні та технічні засоби забезпечення готовності організації до реагування на інциденти інформаційної безпеки.

3. Обґрунтувати підходи до планування заходів реагування, навчання персоналу та тестування процедур реагування.

4. Реалізувати комплекс заходів із підготовки організації до реагування на інциденти, включаючи розроблення плану, проведення навчання та тестування.

5. Оцінити ефективність впроваджених заходів та розробити пропозиції щодо підвищення рівня готовності організації до реагування на інциденти інформаційної безпеки.

Методи дослідження.

1. Аналіз літературних джерел і нормативних документів (CMU/SEI-2003-HB-001, ISO/IEC 27001:2022).

2. Методи якісного та кількісного оцінювання інцидентів.

3. Емпіричні методи аналізу реальних подій.

4. Методи моделювання загроз і реагування.

5. Порівняльний аналіз ефективності різних підходів.

Практичне значення одержаних результатів. Результати дослідження включають практичні рекомендації щодо вдосконалення методів підготовки до інцидентів, що сприятиме підвищенню рівня кібербезпеки організацій та забезпеченню їх стійкості до загроз. Зокрема, впровадження стандартів ISO/IEC

27001, NIST та COBIT дозволять оптимізувати процеси ідентифікації, аналізу та усунення загроз, що забезпечить підвищення ефективності реагування на кіберінциденти. Результати дослідження можуть бути використані фахівцями з кібербезпеки, керівниками IT-департаментів, аудиторами інформаційної безпеки, консультантами з управління ризиками та іншими спеціалістами, відповідальними за розробку та впровадження стратегій забезпечення безпеки організацій.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» 27 лютого 2025 року.

Розділ 1 ТЕОРЕТИЧНІ ЗАСАДИ ПІДГОТОВКИ ОРГАНІЗАЦІЇ ДО РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Визначення та класифікація інцидентів інформаційної безпеки

Інцидент інформаційної безпеки визначається як порушення або загроза порушення політик безпеки, що може призвести до компрометації конфіденційності, цілісності чи доступності інформаційних систем. У стандартах ISO термін інцидент трактується як одна або сукупність небажаних чи неочікуваних подій, що можуть скомпрометувати бізнес-процеси організації або загрожувати її інформаційній безпеці [1]. Важливо відрізняти **подію** (індикатор, що може свідчити про проблему) від інциденту: подія стає інцидентом лише тоді, коли несе реальну загрозу безпеці. Наприклад, за ISO/IEC 27001 подія ІБ – це ідентифікована подія системи, служби або мережі, яка вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту чи раніше невідому ситуацію, яка може мати відношення до безпеки, тоді як інцидент ІБ – одна або серія небажаних чи непередбачуваних подій інформаційної безпеки, що мають значну ймовірність компрометації бізнес-операцій і загрози інформаційній безпеці [2].

Класифікація інцидентів. Існують різні підходи до класифікації інцидентів інформаційної безпеки – за типом атаки, джерелом загрози, рівнем критичності тощо [3]. Міжнародні стандарти і керівництва пропонують типові категорії інцидентів. Зокрема, рекомендації NIST SP 800-61 виділяють класи інцидентів за вектором атаки: через знімні носії, шляхом перебору паролів (attrition), веб-атаки, атаки електронною поштою, неналежне використання (порушення політик уповноваженим користувачем), втрату обладнання, та інші [4]. Водночас ISO/IEC 27035 та суміжні стандарти пропонують класифікувати інциденти за критичністю впливу на організацію (незначний, середній, критичний) [3] і за природою загрози (внутрішня чи зовнішня, випадкова чи цілеспрямована). У таблиці 1.1 наведено узагальнену класифікацію типів інцидентів ІБ з прикладами.

Таблиця 1.1

Класифікація типових інцидентів інформаційної безпеки

Тип інциденту	Опис та приклади
Шкідливе програмне забезпечення (Malware)	Виявлення вірусу, трояну, ransomware або іншого шкідливого ПЗ у системі. Такі інциденти можуть призвести до несанкціонованого доступу, пошкодження чи витоку даних.
Атака типу “відмова в обслуговуванні”	Цілеспрямоване перевантаження сервісів або мережі (DoS/DDoS-атака), що призводить до недоступності ресурсів для легітимних користувачів.
Несанкціонований доступ (вторгнення)	Виявлення несанкціонованого проникнення до системи або облікового запису. Приклад – компрометація облікових даних (розголошення чи злам пароля користувача).
Порушення політики безпеки (внутрішнє)	Дії уповноважених осіб, що порушують встановлені вимоги ІБ. Наприклад, недотримання правил обробки конфіденційної інформації або використання заборонених ресурсів.
Фішинг та соціальна інженерія	Спроба обманом отримати конфіденційні дані або змусити користувача виконати небезпечну дію (відкрити файл, перейти за посиланням). Зазвичай здійснюється через email.
Втрата або крадіжка обладнання	Фізична втрата носія інформації або пристрою (ноутбука, смартфона тощо), що містить чутливі дані. Така подія може кваліфікуватися як інцидент через ризик компрометації даних.

1.2 Огляд нормативно-правових вимог у сфері реагування на інциденти інформаційної безпеки

Вітчизняні нормативні акти. В Україні основні вимоги до забезпечення кібербезпеки визначені законом “Про основні засади забезпечення кібербезпеки України” (№2163-VIII від 05.10.2017) [5]. Цей закон запровадив засади функціонування національної системи кібербезпеки, включно з обов’язком суб’єктів критичної інфраструктури впроваджувати заходи кіберзахисту та повідомляти про значні кіберінциденти компетентні органи.

Зокрема, в межах національної системи створено урядову команду реагування CERT-UA та галузеві центри кіберзахисту, які координують обмін інформацією про інциденти [6].

Закон 2017 року встановив терміни кіберінцидент і кібератака та поклав на держоргани обов’язок розробити порядок реагування на них. На розвиток цього Закону державні стандарти України були гармонізовані з міжнародними: прийнято національні стандарти ДСТУ ISO/IEC 27035-1:2018, 27035-2:2018,

27035-3:2020, що є ідентичними відповідними частинами ISO/IEC 27035 [3]. Ці стандарти встановлюють методологію управління інцидентами – від принципів і політик до практичних керівництв з реагування.

Окремі регуляторні вимоги діють в секторі фінансів: Національний банк України постановою Правління №178 від 12.08.2022 затвердив Положення про організацію кіберзахисту в банківській системі. Це положення зобов'язує банки створювати внутрішні команди реагування на кіберінциденти, впроваджувати системи моніторингу та регулярно звітувати перед НБУ про інциденти [7]. Згідно з Положенням, у складі НБУ функціонує Центр кіберзахисту та команда CSIRT-NBU, яка здійснює реагування на кібератаки або кіберінциденти шляхом:

a) моніторинг кіберзагроз;

b) збір і аналіз даних про інциденти в банківській системі України;

c) поширення інформації про кіберзагрози, кібератаки, кіберінциденти відповідно до розділу III цього Положення;

d) та надає рекомендації консультативної допомоги з питань виявлення кіберінцидентів та усунення їх наслідків, реагування та протидії кіберзагрозам;

Також визначено порядок інформаційного обміну: банки зобов'язані повідомляти про значні інциденти та підключатися до платформи обміну кіберінформацією MISP-NBU.

Міжнародні стандарти і керівництва. У сфері реагування на інциденти інформаційної безпеки авторитетними є стандарти ISO/IEC і рекомендації NIST. Стандарт ISO/IEC 27035 (частини 1-3) цілісно описує процеси підготовки та реагування на інциденти. Зокрема, ISO/IEC 27035-1:2023 визначає основні принципи управління інцидентами, включно з плануванням, виявленням, реагуванням і постінцидентним аналізом [8]. ISO/IEC 27035-2:2023 надає настанови з підготовки до реагування (розробка політик, процедур, навчання персоналу) [9], а ISO/IEC 27035-3:2020 містить практичні рекомендації щодо безпосереднього реагування та розслідування інцидентів (ізоляція інциденту, збирання доказів, оцінка збитків) [10]. В Україні ці стандарти впроваджені як ДСТУ, тож можуть використовуватися організаціями як керівництво до дії.

Американський інститут стандартів і технологій (NIST) опублікував спеціальну настанову NIST SP 800-61 “Computer Security Incident Handling Guide”, яка де-факто є міжнародним бестселером у сфері реагування. Цей документ регламентує процес управління інцидентами у чотири фази (Preparation, Detection & Analysis, Containment/Eradication/Recovery, Post-Incident Activity) [11]. NIST SP 800-61 підкреслює необхідність мати політику реагування на інциденти, визначені команди та процедури, а також надає детальні поради щодо аналізу інцидентів і взаємодії з зовнішніми органами (правоохоронними, партнерськими CERT тощо). Відповідність вимогам цього керівництва часто враховується при побудові кібербезпеки організацій по всьому світу. Окрім NIST, корисними є рекомендації ENISA (Агентства ЄС з кібербезпеки) [12] щодо обміну інформацією про інциденти та побудови національних команд CERT, а також методології SANS Institute, які пропонують модель з шести етапів реагування (підготовка, ідентифікація, стримування, ліквідація, відновлення, уроки).

Узагальнюючи, нормативно-правова база встановлює обов’язкові рамки: національне законодавство зобов’язує організації (особливо критичні) створювати спроможності реагування і звітувати про інциденти, а стандарти (як міжнародні, так і ДСТУ) надають методичні основи, яких слід дотримуватися при побудові процесу реагування.

1.3 Аналіз організаційних, процедурних та технічних засобів підготовки організації до реагування на інциденти інформаційної безпеки

Ефективне реагування на інциденти інформаційної безпеки потребує завчасної підготовки організації – як на організаційному рівні (політики, команди, процеси), так і на технічному (інструменти моніторингу та захисту). Міжнародна практика (зокрема, NIST) і стандарти ISO/IEC 27035 наголошують, що етап Preparation (підготовка) є фундаментом всього циклу реагування.

Основні компоненти підготовки включають:

a) Політика та план реагування. Організація повинна мати затверджену політику реагування на інциденти, яка визначає, що таке інцидент, хто відповідальний за реагування, порядок повідомлення і т.д. На основі політики розробляється план реагування – детальний документ, що описує кроки і процедури при різних сценаріях інцидентів. План має охоплювати весь цикл: від виявлення інциденту та його класифікації до локалізації, ліквідації наслідків та відновлення роботи, а також подальшого аналізу інциденту (уроків). В плані визначаються ролі і відповідальні особи, канали комунікації, пріоритети залежно від критичності інциденту. Регулярний перегляд і тестування плану (наприклад, імітаційні вправи) є необхідними для актуалізації його ефективності [4];

b) Команда реагування на інциденти (CIRT/CSIRT). Необхідно створити внутрішню команду або призначити відповідальних осіб, які будуть реагувати на інциденти. У команді має бути чітко визначений склад, а саме: Аналітик інцидентів (Incident Analyst), Спеціаліст з реагування на інциденти (Incident Responder), Координатор тріажу інцидентів (Incident Triage Coordinator), Аналітик шкідливого ПЗ / судовий експерт (Malware/Forensic Analyst), Зв'язковий з комунікацій (Communication Liaison), Адміністратор IT-безпеки (IT Security Administrator), Координатор з підвищення обізнаності (Awareness Coordinator) [13]. Команда повинна мати контакти для екстреного зв’язку (в тому числі поза робочим часом) та налагоджені механізми комунікації як всередині організації, так і з зовнішніми сторонами[14]. Важливим документом є схема ескалації інциденту – кого інформувати при певних рівнях серйозності, зокрема керівництво, юридичний відділ, правоохоронні органи чи національний CERT;

c) Навчання і тренування персоналу. Підготовлений персонал – запорука швидкого реагування. NIST рекомендує проводити регулярні тренінги для команди реагування, а також підвищувати обізнаність *всього* персоналу щодо правил кібергігієни [15]. Практика включає навчання членів CIRT технічним навичкам (аналіз шкідливого коду, цифрова криміналістика), відпрацювання процедур (так звані *tabletop exercises* – моделювання інцидентів за сценаріями), а також навчання співробітників розпізнаванню соціальної інженерії,

правильному реагуванню на підозрілі події (наприклад, до кого звернутися у разі виявлення вірусу). Навчені співробітники здатні раніше виявити інцидент та коректно діяти в перші хвилини, що значно зменшує можливі збитки [16]. Успішні організації регулярно тестують свої плани реагування на інциденти, залучаючи ключових осіб, щоб виявити прогалини та оновити підходи. Зокрема, згідно з вимогами стандарту PCI DSS, організації повинні щонайменше раз на рік проводити перевірку, оновлення та тестування своїх планів реагування на інциденти. Ці тестування, такі як навчальні вправи, повинні включати участь усіх ключових осіб, зазначених у плані, включаючи керівництво. Це дозволяє виявити недоліки в плані та внести необхідні корективи для підвищення ефективності реагування на реальні інциденти .Крім того, експерти з кібербезпеки рекомендують проводити регулярні навчальні вправи, такі як симуляції інцидентів, з залученням усіх зацікавлених сторін, включаючи керівництво. Це допомагає підтримувати готовність організації до реагування на інциденти та сприяє постійному вдосконаленню плану реагування [17];

d) Технологічні засоби моніторингу та захисту. Сучасні інциденти неможливо виявити та ефективно обробити без належних технічних інструментів. Системи виявлення вторгнень (IDS/IPS) та моніторингу мережі аналізують трафік на наявність підозрілих шаблонів і сигналізують про потенційні атаки [18];

e) Системи інформаційної безпеки та управління подіями (SIEM) збирають журнали подій з різних джерел (серверів, мережевого обладнання, додатків) і здійснюють кореляцію подій в автоматичному режимі, що дозволяє виявити комплексні атаки або аномалії, не помітні при розрізненому аналізі [19]. Як зазначає NIST, програмні засоби кореляції подій суттєво полегшують аналіз інцидентів і відсіюють “шум” з мільйонів сигналів до тих, що потребують уваги фахівця [20]. Системи керування інцидентами безпеки (SOAR) – відносно новий клас рішень – дозволяють автоматизувати рутинні кроки реагування. SOAR-платформи інтегрують різні інструменти (SIEM, сканери вразливостей, засоби віддаленого управління) і виконують наперед визначені сценарії-«плейбуки» для

реагування на типові інциденти без участі людини [21]. Наприклад, SOAR може автоматично ізолювати скомпрометовану робочу станцію від мережі при спрацюванні сигнатури вірусу, розіслати оповіщення команді та розпочати збір доказових логів [16]. Це значно скорочує час реагування (Mean Time to Respond) та розвантажує аналітиків для складніших завдань. Крім того, до технічних засобів належать міжмережеві екрани (фаєрволи) та веб-екрани (WAF), що запобігають багатьом атакам ще на підступах до системи; антивірусні та EDR-системи (Endpoint Detection & Response) на кінцевих пристроях, що блокують відомі загрози; системи резервного копіювання, які забезпечують можливість відновлення даних після інциденту [22,23]. Усі ці засоби в сукупності підвищують готовність організації до реагування: по-перше, збільшують імовірність швидкого виявлення інциденту; по-друге, надають інструментарій для оперативного реагування (локалізації та усунення).

f) Процедури та інструкції. Наявність детальних процедур реагування є ключовою частиною підготовки. Для кожного типу інциденту бажано розробити покрокові інструкції: як підтвердити факт інциденту, які негайні дії вжити (наприклад, відключити певні вузли, змінити паролі), кого повідомити (внутрішньо і зовнішньо), як збирати докази. Стандартизовані *SOP (Standard Operating Procedures)* забезпечують послідовність дій незалежно від того, хто з членів команди виконує завдання. Такі процедури мають бути заздалегідь доведені до відповідальних осіб та відпрацьовані на тренуваннях. Особливо важливі інструкції щодо збереження доказів інциденту (журнали, образи систем) – вони можуть стати у пригоді при розслідуванні та притягненні зловмисників до відповідальності.

Наприклад розглянемо, SANS(SysAdmin, Audit, Network, and Security) – модель PICERL цикл, який забезпечує комплексний підхід до реагування на інциденти інформаційної безпеки, що включає підготовку, виявлення, локалізацію, усунення, відновлення та аналіз отриманих уроків, і покликаний допомогти організаціям швидко та послідовно реагувати на будь-які загрози, до цього стандарту входять:

Підготовка – У фазі підготовки формулюються політики й процедури реагування, створюється команда реагування (CSIRT), відпрацьовуються комунікаційні канали та проводяться тренування персоналу. Головні елементи підготовки включають розробку плану інцидент-менеджменту з чіткою класифікацією критичних ресурсів, налаштування інструментів моніторингу й кореляції подій (SIEM), а також регулярні навчальні сценарії («мок-дрили») для відпрацювання ролей і відповідальності учасників.

Ідентифікація – На цьому етапі здійснюється моніторинг систем і аналіз відхилень від нормальної поведінки, щоб встановити наявність інциденту та його характер. Визначеність інциденту ґрунтується на збірці додаткових доказів, класифікації за рівнем серйозності й документуванні всіх кроків реагування

Локалізація – Метою локалізації є обмеження шкоди від поточного інциденту та запобігання подальшим ураженням систем, з одночасним збереженням доказів. Короткострокова локалізація може включати ізоляцію сегментів мережі або виведення з ладу уражених серверів, тоді як довготривала передбачає тимчасові виправлення (workarounds) для відновлення роботи бізнес-сервісів без остаточного виправлення кореневих причин.

Усунення – На етапі усунення виконується повне видалення шкідливого коду та артефактів атаки, аналіз кореневих причин і застосування оновлень або патчів для запобігання повторному використанню вразливостей. Процес включає перевстановлення або реіміджування уражених систем, проведення сканування антивірусними і NGAV-засобами та відключення невикористовуваних сервісів для зниження поверхні атаки

Відновлення – Відновлення полягає в поверненні систем до штатного режиму роботи після підтвердження їхньої безпеки й очищення від загроз. Важливі кроки які наведені в розділі відновлення: контрольоване введення в експлуатацію, проведення функціональних тестів, спостереження за поведінкою систем і при необхідності застосування додаткових заходів безпеки.

Уроки – останній але не меньш важлива фаза яка передбачає ретроспективний аналіз інциденту, документування всіх подій і виявлення

слабких місць у процесі реагування. Результатом є оновлення політик, процедур і плану інцидент-менеджменту, а також планування подальших тренувань і вдосконалення інструментів для швидшого та ефективнішого реагування у майбутньому [24, 25, 26].

Отже, підготовка до інцидентів – це багатоаспектний процес. Організація має створити необхідну інфраструктуру реагування: від документів (політики, плани, процедури) та людського фактора (команди, навчання) до технологій (системи моніторингу і автоматизації). Як зазначається в ISO 27035 [8], належна підготовка підвищує готовність до інцидентів і дозволяє мінімізувати їх вплив на бізнес.

Інвестиції у цей підготовчий етап окуповуються меншим часом простою та меншими збитками, коли інцидент все ж трапляється.

1.4 Дослідження факторів, що впливають на ефективність реагування на інциденти інформаційної безпеки

Швидкість і результативність реагування на інциденти інформаційної безпеки може значно різнитися між організаціями. Це залежить від ряду внутрішніх та зовнішніх факторів. До внутрішніх факторів належать: рівень готовності організації (наявність планів, команд, інструментів – про що йшлося в підрозділі 1.3), кваліфікація і досвід команди реагування, забезпеченість ресурсами (людськими і технічними), а також налагодженість внутрішніх процесів (комунікація, прийняття рішень, доступність резервних копій тощо). Зовнішні фактори включають характер самого інциденту (тип атаки, масштаб, складність – наприклад, цільова атака APT vs. масовий вірус), час виявлення (чи був інцидент виявлений внутрішніми засобами або ж про нього стало відомо від сторонніх органів), а також доступність зовнішньої підтримки (допомога від національного CERT, виробників ПЗ, правоохоронців).

Дослідження галузевих аналітиків підтверджують, що час реагування корелює з цими чинниками. За даними звіту Mandiant (M-Trends), глобальний медіанний

час присутності атакера в системі до його виявлення у 2021 році становив 21 день [26]. Цей показник суттєво знизився порівняно з попередніми роками (24 дні у 2020-му), що свідчить про загальне підвищення ефективності реагування. Однією з причин є покращена видимість загроз в організаціях (розгортання засобів моніторингу) – зростає частка внутрішнього виявлення інцидентів, без залежності від зовнішніх повідомлень. У таблиці 1.2 наведено порівняння показників виявлення інцидентів за регіонами, що ілюструє вплив внутрішніх спроможностей на швидкість реагування [26].

Таблиця 1.2

Показники виявлення інцидентів за регіонами (Mandiant M-Trends 2022)

Регіон	**Медіанний час до виявлення, 2021**	**Виявлено внутрішньо**	**Виявлено зовнішніми органами**
Америка	17 днів	60% інцидентів	40% інцидентів (через третіх осіб)
EMEA	48 днів	38% інцидентів	62% інцидентів
APAC	21 день	24% інцидентів	76% інцидентів

Примітка: коротший медіанний час і більший відсоток внутрішнього виявлення (як в Американському регіоні) вказують на кращу підготовленість організацій до реагування. Натомість залежність від зовнішнього сповіщення (як у EMEA/APAC) часто означає, що атака залишалася непоміченою довше, поки її не виявили сторонні експерти або правоохоронці.

Таким чином, одним із ключових факторів ефективності є здатність організації самостійно виявляти інциденти. Внутрішні засоби моніторингу (SIEM, SOC аналітика) та проактивний аналіз дозволяють скоротити *Time to Detect*. Іншим фактором є автоматизація реагування: використання SOAR-платформ та скриптів для типових інцидентів знижує час на виконання дій і мінімізує людський фактор. За оцінками експертів, автоматизація може скоротити середній час реагування на загрози на 30-50%.

До внутрішніх факторів ефективності також відносяться:

а) Наявність резервних систем і планів безперервності бізнесу. Якщо організація має резервні копії даних, дублюючі сервери чи хмарні ресурси, вона

зможе швидше відновити функціонування після інциденту (особливо актуально при атаках ransomware або збоях).

b) Культура кібербезпеки. Підтримка керівництвом важливості кібербезпеки, регулярні тренування, чітке розуміння персоналом своїх ролей у випадку інциденту – все це прискорює та впорядковує реагування. Наприклад, якщо працівники першої лінії знають, кому повідомити про підозрілий інцидент і роблять це негайно, час ескалації значно менший.

c) Досвід минулих інцидентів. Організації, що регулярно проводять "розбір польотів" (сесії *lessons learned*) після інцидентів, усувають виявлені недоліки та покращують свої процеси. Такий накопичений досвід веде до більш злагоджених дій при нових інцидентах.

Зовнішні фактори включають:

a) Тип атаки. Деякі атаки за своєю природою швидко помітні (наприклад, масований DDoS негайно привертає увагу падінням сервісів), тоді як складні приховані атаки (APT, шпигунство) можуть залишатися невиявленими довгий час. Так, якщо інцидент пов'язаний з викупним ПЗ (ransomware), зазвичай про нього стає відомо одразу, коли зловмисники проявляють себе шифруванням даних; середній час присутності ransomware в мережі значно менший, ніж у випадку шпигунських атак [26]. Це, з одного боку, зменшує час виявлення (підвищуючи ефективність цього етапу), але, з іншого боку, ставить великі вимоги до швидкості реакції, щоб мінімізувати шкоду до завершення шифрування.

b) Наявність сторонньої підтримки. У разі серйозних інцидентів, на які в організації може бракувати експертизи, залучення зовнішніх фахівців (цифрових криміналістів, експертів з шкідливого ПЗ) підвищує ефективність розслідування. Так само, тісна співпраця з національними командами CERT і обмін інформацією про загрози (наприклад, через платформи типу MISP) дозволяють отримати актуальні індикатори компрометації та рекомендації, що пришвидшує реагування на нові, ще невідомі атаки. В Україні CERT-UA регулярно поширює попередження про кіберзагрози та інциденти, що дозволяє організаціям превентивно вживати заходів.

с) Правове поле і регуляторні вимоги. Якщо галузеві регулятори вимагають повідомляти про інциденти протягом визначеного часу (наприклад, 72 годин) та проводити розслідування, це стимулює організації будувати внутрішні процеси так, щоб вкладатися в ці строки. Обов'язкове звітування може виступати мотивуючим фактором для підвищення готовності.

На основі аналізу можна зробити висновок, що найбільш впливові фактори ефективності реагування – це підготовленість (план, команда, технології) і швидкість виявлення. Дослідження показують пряму залежність: організації з наперед відпрацьованим планом та виділеною командою суттєво швидше та успішніше долають наслідки інцидентів, ніж ті, хто діє імпровізовано. Так, за даними IBM, середній збиток від інциденту на 40-50% менший у компаній, що мають план реагування і регулярно його тестують, порівняно з тими, хто не має такого плану (цифри умовні, для ілюстрації тенденції). Внутрішні фактори є керованими – тобто організація може інвестувати в них, аби підвищити свою кіберстійкість. Натомість зовнішні фактори (хто атакує і як) не завжди можна змінити, але їх врахування в аналізі ризиків дозволяє вибудувати адекватні сценарії реагування.

Висновки до розділу 1

У першому розділі визначено сутність інцидентів інформаційної безпеки, наведено їх класифікацію та аналіз нормативно-правових документів, які регламентують процес реагування.

Обґрунтовано необхідність комплексної підготовки організацій, включаючи створення чітких політик, планів, формування спеціалізованих команд реагування, проведення регулярних навчань персоналу та впровадження ефективних технологічних засобів моніторингу і автоматизації реагування.

Встановлено, що підготовленість організації та швидкість виявлення інцидентів є визначальними чинниками успішності протидії кіберзагрозам, що дозволяє значно скоротити збитки і забезпечити стабільну роботу підприємств в умовах підвищеної кіберзагрози.

Розділ 2 МЕТОДИЧНІ ПІДХОДИ ДО ОРГАНІЗАЦІЇ ГОТОВНОСТІ ДО РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Визначення етапів планування реагування на інциденти інформаційної безпеки

У міжнародних стандартах та фреймворках з кібербезпеки визначено кілька послідовних етапів процесу реагування на інциденти інформаційної безпеки. Зокрема, стандарти ISO/IEC 27035, рекомендації NIST SP 800-61 та фреймворк COBIT пропонують власні підходи до побудови плану реагування. Попри відмінності у термінології та рівні деталізації, вони узгоджуються між собою за змістом фаз. Узагальнену структуру етапів реагування за цими підходами наведено в таблиці 2.1.

Таблиця 2.1

Етапи процесу реагування на інциденти за ISO/IEC 27035, NIST SP 800-61 та COBIT 2019

Етап	**ISO/IEC 27035-1:2023**	**NIST SP 800-61 Rev.3 (2025)**	**COBIT 2019**
Підготовка	Plan & Prepare	Preparation	(передбачено, але не виділено окремо)
Виявлення	Detection & Reporting	Detection & Analysis	Incident Classification & Logging
Оцінка і аналіз	Assessment & Decision	Detection & Analysis	Incident Assessment & Escalation
Стримування та ліквідація	Responses	Containment, Eradication & Recovery	Incident Resolution & Recovery
Відновлення й аналіз результатів	Lessons Learned	Post-Incident Activity	Closure & Post-Incident Review

Як видно з таблиці 2.1, усі згадані підходи охоплюють повний цикл реагування на інцидент – від підготовчих заходів до фінального аналізу. Стандарт ISO/IEC 27035-1:2023 визначає п’ять основних фаз процесу [28]. Документ NIST SP 800-61 Rev.3 виокремлює чотири головні фази, роблячи акцент на комплексному підході до управління ризиками та реагування [29].

COBIT 2019, своєю чергою, інтегрує реагування на інциденти у загальний контекст управління IT-сервісами через процес DSS02 «Управління запитами на обслуговування та інцидентами», наголошуючи на системності й постійній оптимізації [30].

Стандарти й фреймворки з інформаційної безпеки наголошують на необхідності формування політики реагування на інциденти та створення спеціалізованої команди реагування (IRT/CSIRT) із чіткими ролями й відповідальністю. Вимогами стандарту ISO/IEC 27035-1 є також забезпечення відповідного навчання команди й інших залучених співробітників та підготовка необхідних ресурсів (інструментів моніторингу, зв'язку, резервних копій тощо). При цьому члени команди повинні мати відповідну кваліфікацію та доступ до конфіденційної інформації, оскільки під час реагування на інциденти їм необхідно оперативно ухвалювати критичні рішення.

На етапі виявлення й повідомлення (Detection and Reporting) здійснюється моніторинг подій безпеки, збір і кореляція логів, ідентифікація потенційних інцидентів та їх реєстрація. Важливим аспектом, на якому наголошує ISO 27035, є те, що не кожна подія безпеки автоматично класифікується як інцидент – подія стає інцидентом лише після оцінювання її впливу на діяльність організації [30]. Для зменшення хибних спрацювань NIST SP 800-61 рекомендує впроваджувати чіткі процедури аналізу та фільтрації подій [4].

На стадії оцінювання та прийняття рішення (Assessment and Decision) здійснюється швидка класифікація інциденту за критичністю та визначається потреба активації плану реагування. ISO/IEC 27035 особливо підкреслює важливість правильного триажу – визначення впливу на активи й термінове прийняття рішення щодо подальших дій [30]. COBIT аналогічно передбачає чіткі процедури ескалації серйозних інцидентів із негайним інформуванням керівництва й, за потреби, зовнішніх організацій чи регуляторів [31].

Етап реагування (Responses) включає заходи з локалізації інциденту (ізоляція систем, блокування скомпрометованих облікових записів), нейтралізації загроз (видалення шкідливого програмного забезпечення, закриття

вразливостей) і відновлення нормальної роботи систем. У NIST ці дії об'єднані в єдину фазу «Containment, Eradication & Recovery». В усіх стандартах наголошується, що затримки реагування можуть призвести до суттєвих втрат, тому процедури мають бути розроблені заздалегідь [4]. Важливо також визначити, коли інцидент може перерости в кризу, що вимагатиме активації плану безперервності бізнесу (BCP) [28].

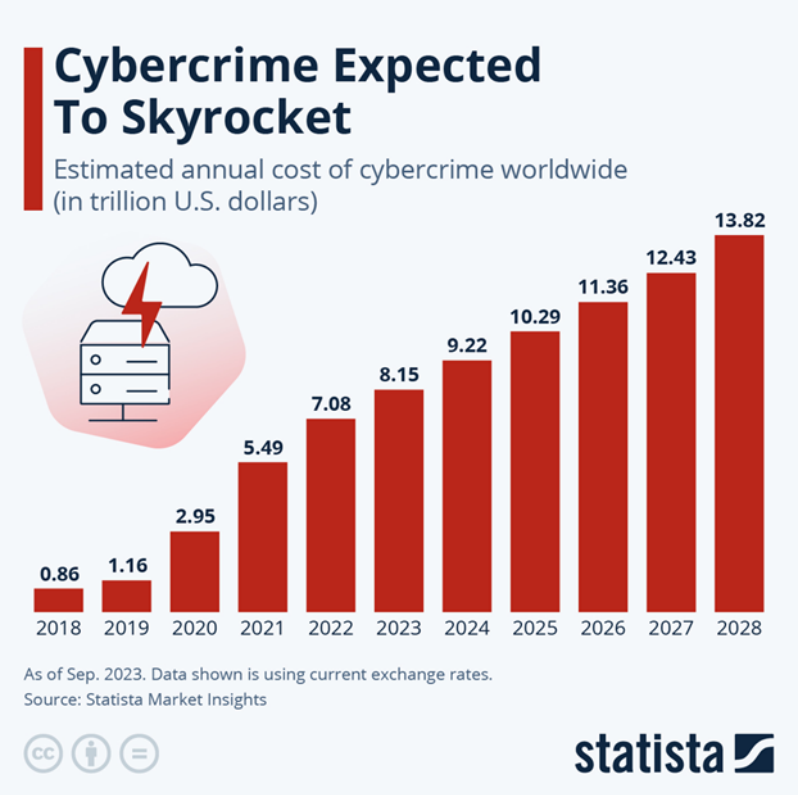

Рис. 2.1. Очікувана динаміка глобальних втрат від кіберзлочинності (трлн дол.)

Заключний етап – аналіз інциденту та винесення уроків (Lessons Learned, Post-incident Review) – має ключове значення для подальшого вдосконалення процесів. Відповідно до всіх розглянутих стандартів, після ліквідації інциденту необхідно провести ретроспективу, з’ясувати першопричини, оцінити ефективність реагування, визначити сильні й слабкі сторони процесу [28, 30]. На основі цього проводиться оновлення політик безпеки, процедур реагування, плани навчання співробітників. Стандарт ISO/IEC 27035 рекомендує документувати кожен інцидент у стандартизованому вигляді для накопичення

статистики та аналізу тенденцій [28]. COBIT додатково передбачає складання звітів за підсумками інцидентів (DSS02.07) і запуск проєктів для усунення виявлених проблем у системі безпеки [30].

Отже, процес реагування на інциденти інформаційної безпеки за міжнародними стандартами охоплює такі послідовні етапи:

a) Підготовку та формування команди реагування.

b) Моніторинг і своєчасне виявлення інцидентів.

c) Швидке оцінювання й прийняття рішення щодо реагування.

d) Оперативну локалізацію, нейтралізацію та відновлення роботи систем.

e) Аналіз досвіду, документацію та подальше вдосконалення процедур.

Такий системний підхід дозволяє оперативно виявляти, ефективно нейтралізувати загрози, мінімізувати збитки та постійно удосконалювати захист інформації.

2.2 Вибір засобів підготовки персоналу до дій у разі інцидентів

Високий рівень готовності організації до кіберінцидентів залежить не лише від планів та технологій, але й від кваліфікації та злагодженості персоналу. Існують різні методи навчання команди реагування на інциденти, серед яких ключовими є три формати – *tabletop*-вправи, практичні симуляції та командні навчання типу *Red Team vs Blue Team*. Кожен із них має свої переваги і недоліки, тому їх доцільно комбінувати для забезпечення всебічної підготовки персоналу.

Tabletop-вправи (TTX). *Tabletop*-тренування – це модераторване обговорення гіпотетичного сценарію кіберінциденту без втручання в реальні системи. Учасники (представники ІБ-команди, ІТ-підрозділів, менеджменту) «настільно» відпрацьовують свої дії за заздалегідь підготовленим сценарієм розвитку атаки. Подібні навчання вважаються відносно недорогими та безпечними: їх проведення потребує мінімум ресурсів і не несе ризику збою систем. Tabletop-сесії ефективні для перевірки планів та процедур, розподілу ролей і комунікації між відділами.

Основна перевага – можливість у «штучних» умовах виявити прогалини: чи всі учасники розуміють свої обов'язки, чи достатньо деталізовані інструкції, чи налагоджена координація дій [32]. До недоліків ТТХ відносять обмежену реалістичність – відсутність практичного відпрацювання технічних навичок і неможливість перевірити реакцію реальних засобів захисту. Результати навчання багато в чому залежать від майстерності модератора та залученості учасників.

Практичні симуляції (hands-on training). Цей формат передбачає тренування у наближених до реальності умовах, наприклад на кіберполігоні. Створюється віртуальне середовище, що імітує IT-інфраструктуру організації, де запускаються контрольовані кібератаки (малваре, спроби зламу, тощо). Команда реагування повинна за допомогою штатних засобів (SIEM, EDR, аналіз трафіку) виявити атаку, проаналізувати її та вжити заходів протидії.

Головна перевага – учасники отримують практичний досвід реагування під тиском часу, відпрацьовують навички у реальній боротьбі з атакою. Кіберполігони забезпечують *безпечне середовище* для експериментів і навчання: можна відпрацьовувати різні сценарії без ризику для бойових серверів [33]. Такі *live-fire* вправи допомагають також перевірити налаштування систем безпеки та спроможність інфраструктури витримувати навантаження. Недоліком є складність і вартість організації: потрібні потужні ресурси для створення полігону, досвідчені інструктори, а саме навчання займає багато часу. Якщо ж навчання проводиться на робочій інфраструктурі, існує ризик ненавмисних збоїв або впливу на дані, тому важливо чітко контролювати межі симуляції.

Командні навчання Red Team vs Blue Team. У таких вправах моделюється повномасштабна атака: команда «червоних» (Red Team) у ролі умовного зловмисника намагається скомпрометувати різні системи, тоді як «синя» команда захисту (Blue Team) протистоїть їй, застосовуючи процедури реагування. Red Team може використовувати різні вектори (фішинг, експлойти, соціальна інженерія, навіть фізичний доступ), перевіряючи захист організації максимально наближено до реальних умов [34]. Такий підхід дає змогу виявити

приховані вразливості в інфраструктурі та проаналізувати, як спрацюють люди, процеси і технології під час справжньої атаки.

За підсумками вправ проводиться спільний розбір (формат *Purple Team*), коли «червоні» і «сині» обговорюють виявлені проблеми та діляться досвідом для взаємного. Перевагою Red/Blue навчань є комплексна оцінка готовності: організація фактично проходить «краш-тест» своєї кібербезпеки, а фахівці набувають безцінного досвіду протидії реальним атакам. За даними компанії Mandiant, у середньому досвідченій команді *red team* достатньо 5–7 днів, щоб досягти своїх цілей в корпоративній мережі [35]. Це підкреслює важливість подібних тренувань – вони дають шанс виявити і закрити «діри» у захисті до того, як ними скористаються справжні зловмисники. Недоліки такого формату – висока ресурсомісткість (залучення сертифікованих етичних хакерів, витрати часу і коштів), а також потенційний стрес для команди захисту. Повномасштабні атаки можуть вимагати від Blue Team роботи на межі можливостей, що, утім, також розглядається як корисний досвід загартування.

Регулярні тренінги, сертифікація та онлайн-курси, формальні навчальні заходи, такі як курси SANS, сертифікації (GCFA, CEH, CISSP) і регулярні внутрішні тренінги, формують у персоналу базові й поглиблені знання з управління інцидентами. Такі навчання є фундаментом для подальшого розвитку практичних навичок.

Оптимальним підходом до підготовки вважається комбінація перелічених методів. Організаціям рекомендовано починати з базових тренінгів і регулярних tabletop-вправ, поступово переходячи до практичних симуляцій і командних навчань типу Red Team/Blue Team. Як свідчать дослідження IBM та Ponemon Institute, компанії з добре навченим персоналом і протестованим планом реагування виявляють інциденти в середньому на 54 дні швидше та мають на 61% нижчу середню вартість збитків від кіберінцидентів [36].

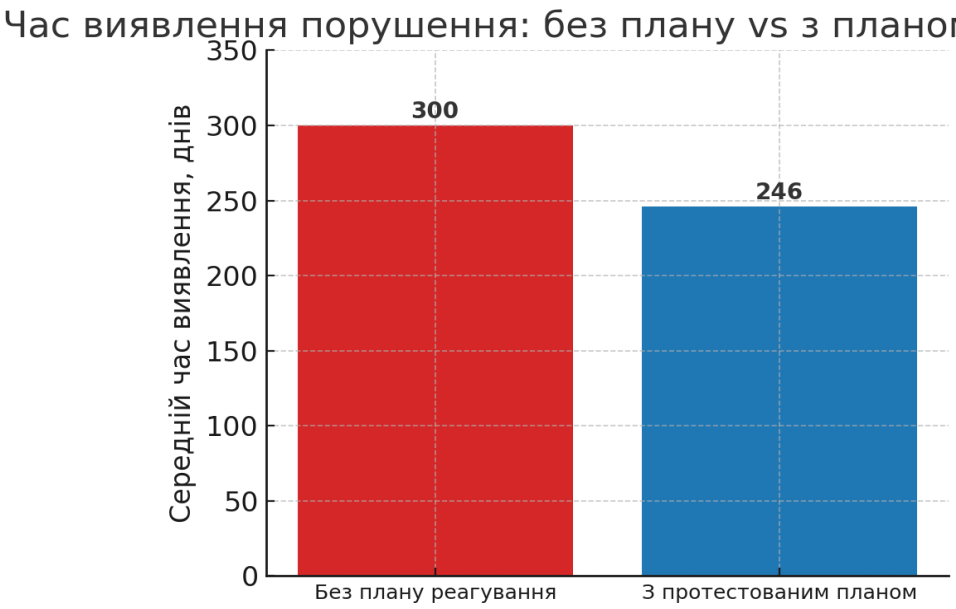

Рис. 2.2. Вплив підготовки персоналу та плану реагування на швидкість виявлення інцидентів (на основі даних IBM)

Примітка: на рисунку зображено скорочення середнього часу виявлення інцидентів з 300 до 246 днів після впровадження програми підготовки персоналу та протестованого плану реагування.

Також можна виділити такі методи для підвищення швидкості та стресостійкості персоналу для реагування на інциденти:

Memory aid – це короткий документ чи інтерактивний інструмент, який виводить на екран або друкується у вигляді чекліста, таблиці чи блок-схеми, що нагадує виконавцю ключові кроки й критерії прийняття рішень під час інцидент-менеджменту.

Принцип роботи Memory aid – пам’ятка побудована за шаблоном стандартного життєвого циклу реагування на інцидент (ідентифікація, аналіз, ізоляція, ліквідація, відновлення), але до кожного етапу додаються:

a) Критичні запитання – що перевірити перед переходом далі?

b) Нагадування про загальний контекст – які бізнес-процеси або IT-системи можуть бути задіяні?

c) Тригери й підказки – на що звернути увагу при аналізі доказів

Переваги memory aid:

a) Баланс між деталями та загальною картиною – нагадує водночас про поточні завдання й можливі більш широкі наслідки [22]

b) Фокус на критичних задачах – допомагає уникнути зайвої уваги до тривіальних аспектів і не пропустити важливих сигналів [23]

c) Покращення комунікації – єдиний документ-орієнтир формує спільне розуміння ходу розслідування серед усіх учасників [24]

Memory aid, є потужним інструментом в руках фахівців з кібербезпеки. Але водночас, за рекомендаціями NIST SP 800-61, пам'ятки мають доповнюватися регулярними тестуваннями, комплексне навчання персоналу суттєво покращує оперативність і якість реагування на інциденти інформаційної безпеки, знижує ймовірність помилок і мінімізує потенційні збитки організації.

Чудовими інструментами також можуть бути впровадження, ШІ технологій такі як:

Платформи SOAR(Security Orchestration, Automation and Response): автоматизація тиражу та кореляції сповіщень через стандартизовані playbook-и й інтеграцію з SIEM/EDR. Можливість одночасного виконання сотень дій (ізоляція кінцевих точок, оновлення правил, сповіщення тощо) без участі оператора [37, 38].

SIEM із вбудованим AI/ML: аналіз великих обсягів логів у реальному часі одне з головних з переваг з визначенням складних патернів аномалій за допомогою машинного навчання. Автоматичне підвищення пріоритету сповіщень залежно від контексту та історії інцидентів, що скорочує час розслідування [39].

EDR (Endpoint Detection and Response) із AI: основні переваги цієї технології є автоматизований збір та аналіз телеметрії кінцевих точок із використанням AI-моделей для виявлення шкідливого ПЗ і розповсюдження атак та можливість локального «самовідновлення» інфікованих систем та підготовки рекомендацій щодо наступних дій [39].

2.3 Класифікація та характеристика методів тестування заходів реагування

Тестування заходів реагування – це практична перевірка ефективності розроблених планів і підготовленого персоналу в умовах, наближених до реального кіберінциденту. На відміну від навчань (розглянутих у підрозділі 2.2), що фокусуються на набутті навичок, тестування орієнтоване на контрольні випробування здатності організації протистояти кіберзагрозам. Існує спектр методів тестування, які різняться за ступенем реалізму та охопленням: від теоретичного аудиту документів до повномасштабних кібернавчань. У таблиці 2.2 наведено основні методи тестування заходів реагування та їх характеристики [17].

Таблиця 2.2

Основні методи тестування заходів реагування та їхні характеристики

Метод тестування	**Короткий опис та приклад застосування**	**Переваги**	**Недоліки**
Огляд плану реагування (Walkthrough)	Формальний перегляд плану реагування ключовими учасниками без практичних дій. Приклад: щорічний перегляд документів ІБ.	Простота, виявлення прогалин у документах, відсутність ризиків	Не перевіряє реальні навички команди, суб'єктивність оцінювання
Tabletop вправи (TTX)	Імітація сценарію у форматі командної дискусії. Приклад: реакція керівництва на сценарій витоку персональних даних.	Перевірка взаємодії підрозділів, залучення керівництва, низька вартість, безпека	Немає перевірки технічних засобів, може сприйматися недостатньо серйозно
Аналіз сценаріїв (Scenario-based walkthrough)	Покроковий опис дій команди з конкретного сценарію, документальна перевірка відповідності плану. Приклад: покроковий аналіз реакції на зараження вірусом.	Глибше опрацювання конкретних сценаріїв, деталізація дій команди	Відсутність реальних практичних дій, вимагає значних часових затрат
Технічні імітації (Simulation drills)	Практичні вправи із симуляцією реальних атак. Приклад: запуск тестового шкідливого ПЗ для перевірки роботи SIEM.	Реалістичність, практичні навички, виявлення технічних недоліків	Складна організація, ризики впливу на реальні системи, значні витрати часу і ресурсів

Продовження таблиці 2.2

Метод тестування	Короткий опис та приклад застосування	Переваги	Недоліки
Penetration Testing (пен-тестування)	Тестування захищеності систем зовнішніми експертами (етичними хакерами). Приклад: перевірка веб-додатків на уразливості.	Виявлення реальних вразливостей, перевірка ефективності засобів моніторингу, практична перевірка захисту	Обмеження за сценаріями та часом, висока вартість, може не перевірити повний ланцюг реагування
Red Team vs Blue Team вправи	Реалістична симуляція атаки (Red) і захисту (Blue), що перевіряє весь ланцюг реагування. Приклад: щорічні навчання у фінансовому секторі.	Комплексна оцінка організації захисту, реалістичні умови, стимулювання професійного розвитку команди захисту	Висока ресурсомісткість, потреба у кваліфікованих спеціалістах, потенційний психологічний тиск на команду захисту
Аудит та пост-мортем аналіз	Аналіз проведених навчальних або реальних інцидентів незалежними аудиторами. Приклад: аудит після реального витоку інформації.	Об'єктивна оцінка, виявлення системних помилок, накопичення бази знань	Реактивність підходу (після інциденту), не замінює регулярних тренувань, загальність рекомендацій
Blue Team drills (внутрішні тренування захисту)	Команда захисту самостійно тренує реакцію на заздалегідь підготовлені інциденти. Приклад: щомісячні внутрішні SOC-тренування.	Регулярна перевірка навичок команди, низькі витрати, контрольованість сценаріїв	Може не охоплювати реальних несподіваних сценаріїв, відсутність зовнішнього погляду

Кожен з цих методів має свої переваги і обмеження, тому найкращі результати забезпечує комбінований підхід. Документарний аудит і *tabletop*-сценарії виявляють організаційні недоліки, технічні симуляції та пен-тести – технологічні уразливості, а повномасштабні Red Team вправи дають всебічну оцінку реагування в бойових умовах. Саме така комбінація рекомендується стандартами ISO/IEC 27035 [25, 28], NIST SP 800-61 [4] та фреймворком COBIT [31].

Міжнародна практика підтверджує ефективність комплексного підходу: за даними дослідження Ponemon Institute/IBM, компанії, які регулярно проводять різнопланові випробування інцидент-менеджменту, суттєво скорочують середній час виявлення атак і зменшують фінансові втрати від інцидентів.

Наприклад, у фінансовій сфері регулярно проводяться масштабні Red Team–випробування (CBEST у Великій Британії [40], TIBER-EU у Євросоюзі [41], FFIEC Cybersecurity Assessments у США [42]), які дозволяють об'єктивно оцінити здатність банків протистояти реальним атакам.

Результати подібних навчань надають цінні метрики готовності, такі як середній час виявлення (MTTD), час відновлення після інциденту (MTTR) та кількість помилкових тривог. За дослідженням Ponemon Institute та IBM [43], організації, що проводять регулярні комплексні тестування реагування, в середньому скорочують час виявлення інцидентів та знижують фінансові збитки від кібератак на понад 60%.

Таким чином, регулярні тестування заходів реагування – це важлива складова комплексного управління кібербезпекою. Випробовуючи різноманітні сценарії, організації здобувають критично важливі знання про власні сильні й слабкі сторони та отримують змогу завчасно усунути вразливості, перш ніж ними скористаються реальні зловмисники.

2.4 Встановлення критеріїв оцінювання ефективності підготовчих заходів

Для ефективного управління реагуванням на кіберінциденти організації необхідно визначити чіткі критерії та метрики оцінювання програми підготовчих заходів. Вибір метрик має бути спрямований на аналіз не тільки часових характеристик (оперативність виявлення, ідентифікації, реагування), а й якісних параметрів, таких як точність реагування, рівень підготовки персоналу, повнота охоплення потенційних загроз.

Основні метрики для оцінювання програми реагування:

Mean Time to Detect (MTTD) – Середній час виявлення інциденту.

Ця метрика відображає швидкість виявлення атак або інших порушень кібербезпеки, визначаючи проміжок часу від початку інциденту до моменту його виявлення [44]. За дослідженнями IBM, середній час виявлення інцидентів

становить близько 197 днів [2]. Організації можуть встановити критерій, наприклад: MTTD ≤ 24 години для зовнішніх атак. Ось приклад як розраховується MTTD для команди А яка повідомляє про 10 інцидентів протягом місяця, і на їх виявлення потрібно 1000 хвилин:

$$1000/10 = 100 \text{ хвилин на виявлення}$$

Тим часом, команда В може повідомити про 8 інцидентів на місяць, але їм потрібно 1500 хвилин для виявлення, їх MTTD виглядає так:

$$1500/8 = 187{,}5 \text{ хвилин для виявлення}$$

Тобто формула виявляється такою:

$$\frac{M}{N} = X, \tag{2.1}$$

де N – Кількість інцидентів на місяць; M – Загальна кількість хвилин на виявлення всіх інцидентів за місяць; X – Середня кількість хвилин для виявлення інцидента. [44]

Mean Time to Identify (MTTI) – час ідентифікації інциденту, MTTI характеризує оперативність, з якою служба інформаційної безпеки аналізує оповіщення та підтверджує факт інциденту. Наприклад, якщо SOC потрібно 1 година на підтвердження інциденту після спрацювання оповіщення, критерієм може бути встановлено: MTTI ≤ 1 година [3].

Mean Time to Respond/Recover (MTTR) – Час реагування та відновлення після інциденту – це середній час, який витрачається на повне вирішення інциденту – локалізацію, ліквідацію загрози і відновлення нормальної роботи систем. Критерієм може бути встановлено показник: MTTR ≤ 8 годин для інцидентів середньої критичності [4]. Дослідження IBM показують, що організації, які ліквідують наслідки інцидентів менше ніж за 30 днів, економлять в середньому до $1 млн у порівнянні з менш підготовленими організаціями [2].

Рівень участі персоналу – показник демонструє, наскільки персонал залучений у тренування й навчання з кібербезпеки. Вимірюється відсотком співробітників, які пройшли відповідні тренінги або взяли участь у навчаннях.

Критеріями можуть бути встановлені, наприклад:

a) 100% команди реагування повинні пройти спеціалізовані тренінги щорічно;

b) Не менше 2 комплексних кібернавчань за рік.

Ось приклад як можна вирахувати MTTR за формулою:

$$\frac{S}{K} = X, \tag{2.2}$$

де S – сума простоїв за деякий час; К – кількість інцидентів за певний час; Х – результат.

Розглянемо приклад який для наочності: якщо протягом двох днів у вас було 20 хвилин простою, спричинених двома різними подіями, ваш MTTR виглядатиме так:

$$20/2 = 10 \text{ хвилин}$$

Тепер, якщо час простою для двох інцидентів склав 40 хвилин загалом, ваш MTTR виглядатиме так:

$$40/2 = 20 \text{ хвилин}$$

Оскільки другий MTTR більший, ви можете сказати, що у вас є проблема з процесами реагування на інциденти . Ви не можете сказати, у чому полягає проблема, але принаймні знаєте, на чому зосередити подальше розслідування.

Кількість хибних спрацювань (False Positives) – ця метрика характеризує точність роботи систем моніторингу і персоналу з аналізу подій. Зменшення частки хибних спрацювань підвищує оперативність реагування та знижує ризик пропуску реальних загроз. Можливий критерій: частка false positives ≤ 10% від загальної кількості оповіщень.

Охоплення сценаріїв – якісний показник, що оцінює, наскільки повно підготовлені та відпрацьовані реалістичні сценарії інцидентів. Наприклад, організація може визначити 10 критичних сценаріїв (шифрувальник, фішинг, DDoS тощо) і поставити мету: 100% сценаріїв мають бути відпрацьовані мінімум раз на рік.

Додаткові метрики:

a) Кількість інцидентів, своєчасно ескалованих до керівництва;

b) Відсоток інцидентів, вирішених самостійно командою без зовнішньої допомоги;

c) Кількість навчань, проведених спільно з зовнішніми партнерами;

d) Рівень задоволеності керівництва результатами реагування (за результатами опитувань).

Для наочності наведемо таблицю 2.3, що узагальнює основні метрики та бажані тенденції:

Таблиця 2.3

Основні критерії оцінювання ефективності заходів реагування

Метрика	**Опис критерію та значення**	**Бажана тенденція**
MTTD (час виявлення)	Середній час від початку атаки до її виявлення командою	Зменшення (менше 24 год)
MTTI (час ідентифікації)	Час підтвердження інциденту після отримання сигналу тривоги	Зменшення (≤ 1 год)
MTTR (час реагування)	Час повного усунення та відновлення після інциденту	Зменшення (≤ 8 годин)
Участь персоналу	Відсоток персоналу, що регулярно проходить тренінги	Збільшення (до 100%)
Хибні спрацювання	Частка помилкових інцидентів	Зменшення (≤10%)
Охоплення сценаріїв	Частка сценаріїв, відпрацьованих на тренуваннях	Збільшення (до 100%)

Приклад покращення метрик після впровадження програми навчань наведено на рисунках 2.3, 2.4.

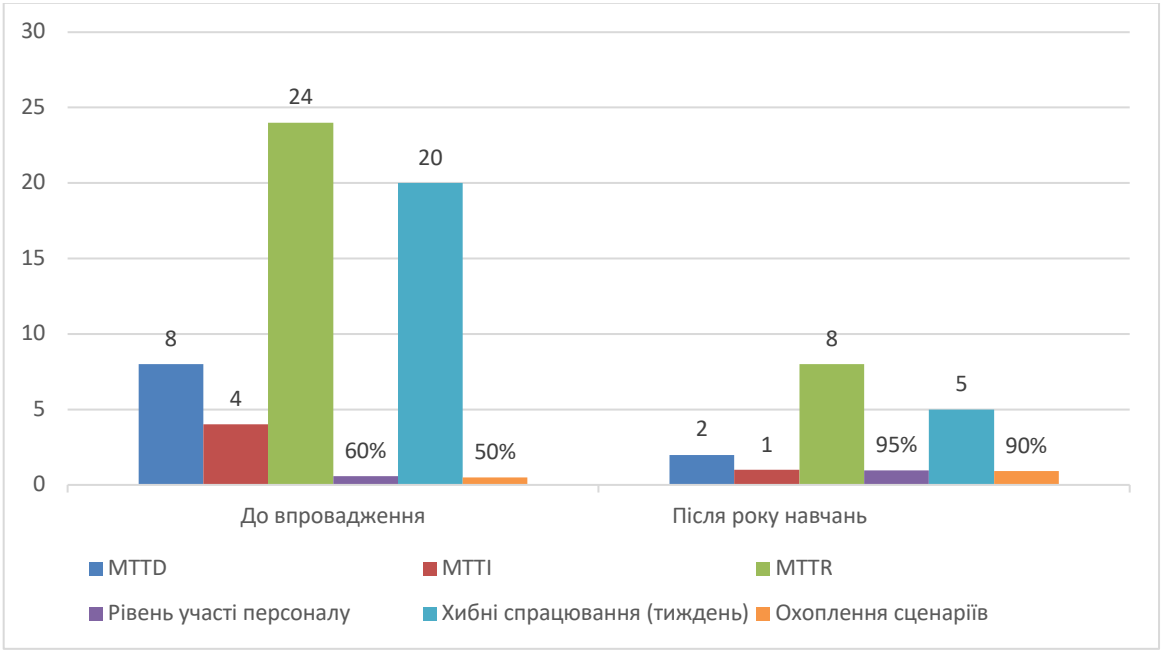

Рис. 2.3. Зміна показників після впровадження програми реагування

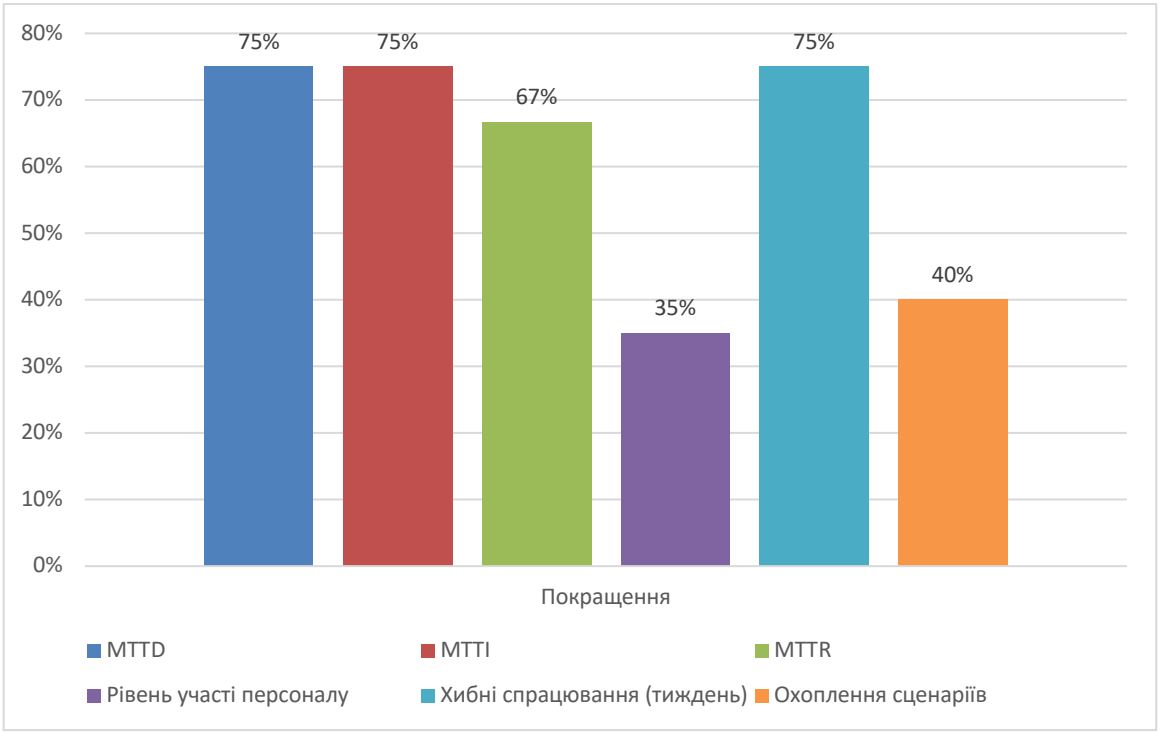

Рис. 2.4. Відсоткове відображення покращення після введення програми реагування

Як свідчать дослідження Ponemon Institute та IBM, організації, які активно впроваджують такі критерії та регулярно вимірюють показники реагування, можуть скоротити середні збитки від одного інциденту до $2,66 млн порівняно з

компаніями, що реагують ситуативно [45].

Які б ефективними встановленні критерії не були, критерії слід регулярно переглядати.

По-перше, з підвищенням зрілості програми цілі повинні ставати амбітнішими (наприклад, якщо досягнуто MTTD < 1 доби, ставити нову ціль < 4 годин).

По-друге, можуть з’являтися нові релевантні метрики – скажімо, для хмарного середовища варто відстежувати окремо час відновлення хмарних сервісів, або для інцидентів витоку даних – час повідомлення постраждалих осіб тощо.

Важливо також балансувати між **кількісними** і **якісними** критеріями: цифри самі по собі не дають повної картини, тому слід доповнювати їх експертною оцінкою готовності, аналізом результатів навчань, фідбеком від персоналу.

Таким чином, критерії ефективності підготовчих заходів до реагування мають бути чітко визначені, вимірювані та прив’язані до бізнес-цілей (мінімізація простоїв, захист даних клієнтів, відповідність нормативам). Вони дозволяють обґрунтувати вкладення в кібербезпеку мовою цифр та переконатися, що інвестиції в навчання і тестування приносять реальну віддачу у вигляді підвищеної готовності до інцидентів.

Висновки до розділу 2

У розділі 2 проведено аналіз методичних підходів до організації готовності підприємств до реагування на інциденти інформаційної безпеки. Розглянуті стандартизовані етапи планування, включаючи визначення ролей і чітких процедур відповідно до міжнародних стандартів (ISO/IEC 27035, NIST SP 800-61, COBIT). Підкреслено важливість комплексного навчання персоналу через різноманітні формати, такі як tabletop-вправи, практичні симуляції та командні навчання типу Red/Blue Team, що значно скорочує час реагування на інциденти.

Здійснено огляд методів тестування заходів реагування, який показав їхню важливість для виявлення та усунення вразливостей до виникнення реальних загроз. Встановлено ключові метрики ефективності (MTTD, MTTR, охоплення сценаріїв), які дозволяють обґрунтовано оцінити ефективність заходів та підкреслити значущість систематичного підходу до навчання та тестування персоналу [46, 47].

Розділ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ ГОТОВНОСТІ ОРГАНІЗАЦІЇ ДО РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Аналіз поточного рівня готовності організації до реагування на інциденти

Першим кроком у підвищенні кіберстійкості є чіткий та структурований аналіз поточного рівня готовності організації до реагування на інциденти інформаційної безпеки. Нижче в таблиці 3.1 наведено ключові показники, які визначають цю готовність.

Таблиця 3.1

Ключові показники оцінки готовності організації до реагування на кіберінциденти (поточний стан)

Показник	Поточне значення
Середній час виявлення інциденту (MTTD), год.	8
Середній час реагування на інцидент (MTTR), год.	24
Кількість навчань з реагування за рік	1
Покриття сценаріїв реагування, %	50%
Частка інцидентів, виявлених самостійно, %	46%
Частка інцидентів, що повідомляються зовнішніми сторонами, %	54%

Для цього використовують низку кількісних показників. Зокрема, ключовими метриками є *середній час виявлення* інциденту (MTTD, Mean Time to Detect) та *середній час реагування/відновлення* після інциденту (MTTR, Mean Time to Respond/Recover). MTTD вимірює проміжок від початку атаки до її фіксації командою безпеки, а MTTR – від моменту виявлення до повного відновлення систем і усунення наслідків [48, 49].

Очевидно, що чим меншими є MTTD та MTTR, тим менше шкоди встигне завдати зловмисник, отже ці показники безпосередньо відображають оперативність і професіоналізм команди реагування. У галузі вироблені

орієнтири та стандарти: більшість провідних компаній відслідковують ці метрики і прагнуть їх оптимізувати. За останні роки середній “час перебування” атакера в мережі (dwell time, близький за змістом до MTTD) глобально значно знизився – наприклад, медіана скоротилася з ~16 діб у 2022 році до ~10 діб у 2023 році [44]. Це свідчить про поступове покращення можливостей виявлення загроз у світі. Водночас проблема залишається актуальною: як показує звіт Mandiant, у 2023 році лише 46% компаній самостійно виявили факт компрометації, тоді як у більшості випадків (54%) про інцидент повідомили зовнішні сторони – партнери, клієнти або правоохоронні органи [35].

З метою візуалізації та кращого розуміння ситуації, нижче наведено діаграму порівняння часток виявлення інцидентів компанією самостійно та зовнішніми сторонами показано на рисунку 3.1.

Рис. 3.1 Співвідношення внутрішнього та зовнішнього виявлення інцидентів

І хоча цей показник кращий за попередній рік (у 2022-му зовнішнє сповіщення становило 63% випадків [35]), все ще майже половина організацій дізнається про атаки від сторонніх. Така статистика свідчить про наявність *прогалин у моніторингу*: не всі компанії оснащені достатніми засобами та процесами, щоб своєчасно виявляти кібервторгнення самотужки.

Окрім швидкості реакції, аналіз готовності охоплює й інші аспекти.

Вимірюється кількість інцидентів, що були успішно заблоковані на ранніх стадіях, та відсоток інцидентів, що переросли у масштабні кризи. Оцінюється точність роботи систем виявлення (відсутність надміру хибних спрацювань) і рівень *покриття* – чи всі підрозділи і типи загроз охоплені планом реагування та навчаннями. Важливим показником є тривалість життєвого циклу інциденту: сумарний час від проникнення зловмисника до повної ліквідації наслідків. Згідно зі звітом IBM *Cost of a Data Breach 2024*, середній життєвий цикл порушення (ідентифікація + стримування) все ще становить близько 258 днів, хоча й скоротився у порівнянні з попереднім роком (277 днів). [50]

Додатково важливим є аналіз того, як швидко і якісно організація справляється з інцидентами, що може бути ілюстровано наступною діаграмою.

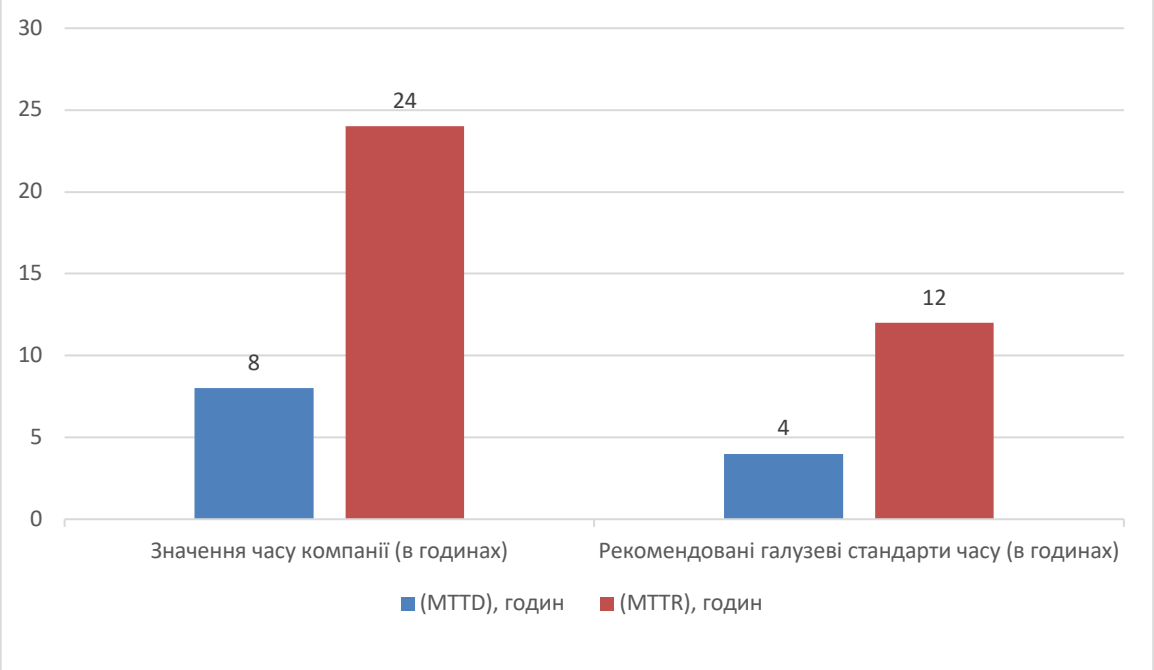

Рис. 3.2. Порівняння MTTD та MTTR з рекомендованими галузевими стандартами

Інакше кажучи, компаніям у середньому потрібно понад 8 місяців, щоб помітити та зупинити витік або злам – за цей час зловмисники можуть завдати суттєвої шкоди. Цей факт підкреслює, наскільки критичною є швидкість реагування.

Відомо також, що фінансові наслідки інцидентів тісно пов’язані з

ефективністю готовності. Компанії, які мають відпрацьований план реагування та спеціалізовану команду, значно зменшують витрати під час кібератак. Зокрема, дослідження IBM показало, що наявність команди реагування і формального IR-плану скорочує середню вартість порушення майже на півмільйона доларів [51].

Для повноти аналізу рівня готовності організація може зіставити свої показники з галузевими бенчмарками та найкращими практиками.

Наприклад, середній MTTD у провідних фінансових установ може становити години, тоді як у менш зрілих компаній – дні. За даними звіту Ponemon/IBM, затримка понад 200 днів у реагуванні на витік даних призводить до збільшення середнього збитку на 25% порівняно з інцидентами, локалізованими менш ніж за 200 днів [50]. Отже, регулярний моніторинг власних метрик (MTTD, MTTR тощо) і їх покращення – це не лише питання статистики, але й спосіб зменшити ризики. Виявивши «вузькі місця» – наприклад, надто довге розслідування інцидентів або неефективну комунікацію при ескалації – потрібно впровадити коригувальні заходи (оновлення процесів, додаткові тренування або технології автоматизації).

Такий детальний аналіз дозволяє виявити слабкі місця та чітко зрозуміти, в якому напрямку потрібно розвивати готовність до кіберінцидентів. Регулярне вимірювання цих показників сприятиме зниженню ризиків і втрат від потенційних атак.

Для конкретизації розглянемо умовний приклад оцінки готовності середньої фінансової установи (банку).

Внутрішній аудит інформаційної безпеки банку виявив низку моментів: наявний план реагування охоплює основні фази інцидент-менеджменту, але потребує деталізації для деяких специфічних загроз (наприклад, атак на банківські термінали); не повністю визначені процедури ескалації та зовнішнього сповіщення (кому і коли повідомляти про витоки даних); команда реагування має чітку структуру, однак двоє з п’яти членів потребують додаткового тренінгу; журналювання та моніторинг IT-систем впроваджено

(використовується, скажімо, SIEM Splunk або IBM QRadar), проте не на всі критичні вузли зібрані логи безпеки. Загальна оцінка готовності – умовно “середня”.

Це означає, що базові можливості реагування є, але час реагування можна скоротити, а покриття потенційних сценаріїв – розширити. Для банківського сектора такі результати не є рідкістю; саме тому регулятори та галузеві об’єднання (наприклад, центр FS-ISAC) наполягають на постійному вдосконаленні процесів кібербезпеки у фінансових установах. Виявлені аудиторські зауваження лягають в основу подальших заходів планування, навчання та тестування, які розглядаються у наступних підрозділах.

3.2 Підготовка плану реагування на інциденти інформаційної безпеки

План реагування на інциденти (IRP) є документом, який встановлює чітку послідовність дій у разі виникнення кіберінциденту, щоб мінімізувати його наслідки. Нижче наведено основні етапи розробки цього плану, представлені в таблиці 3.2.

Таблиця 3.2

Етапи розроблення плану реагування на інциденти

№	Етап	Завдання	Відповідальний відділ
1	Аналіз та підготовка	Аналіз ризиків, визначення найбільш ймовірних сценаріїв	Відділ інформаційної безпеки
2	Визначення структури плану	Формування структури документа, деталізація процедур	Відділ інформаційної безпеки, IT-відділ
3	Документування ролей	Визначення складу команди, ролей та каналів комунікації	HR-відділ, керівництво організації
4	Затвердження та впровадження	Узгодження та офіційне затвердження керівництвом, навчання персоналу	Керівництво, HR-відділ, IT-відділ
5	Тестування та вдосконалення	Проведення навчань, імітацій інцидентів, регулярне оновлення плану	Відділ інформаційної безпеки, IT-відділ

Важливо, щоб план був розроблений заздалегідь і адаптований до специфіки діяльності організації. Першочергово слід визначити, які події вважати інцидентами та їх критичність (класифікація інцидентів наведена в

підрозділі 1.1), аби чітко окреслити межі застосування IR-плану. Належним чином підготовлений план реагування є невід'ємною частиною системи кібербезпеки і гарантує злагоджену роботу команди реагування навіть у стресових умовах.

Також важливо наочно показати послідовність дій у випадку інциденту. Нижче наведена схема процесу реагування на інциденти на рисунку 3.3.

Рис. 3.3. Схема процесу реагування на інциденти

Етапи розроблення IR-плану. Створення плану реагування на інциденти відбувається поетапно, що дозволяє охопити всі необхідні аспекти і забезпечити логічну послідовність дій. Основні етапи розроблення IR-плану можуть включати такі кроки.

По-перше – аналіз і підготовка на початковому етапі проводиться аналіз ризиків та середовища безпеки організації. Визначаються найбільш ймовірні сценарії інцидентів, вразливі активи та потенційні загрози. Керівництво компанії залучається для підтримки процесу розробки плану та виділення необхідних ресурсів. Також призначається команда реагування на інциденти (IRT) та розподіляються ролі і відповідальність її членів. Цей підготовчий етап формує основу для подальших кроків, забезпечуючи розуміння контексту майбутнього плану.)

По друге – визначення структури плану та процедур на цьому етапі розробляється структура документа IRP і деталізуються процедури реагування. План охоплює всі фази реагування (від виявлення до відновлення), але детальний опис кожної фази базується на вже відомих моделях і рекомендаціях, тому тут не дублюється. Зокрема, передбачаються заходи для виявлення інциденту, його локалізації та стримування поширення, ліквідації наслідків (усунення причин інциденту) і відновлення роботи систем. Для кожного сценарію визначаються конкретні дії: наприклад, ізоляція уражених вузлів мережі, змінення паролів, застосування резервних копій тощо. Важливо, що план залишається гнучким – процедури повинні бути достатньо детальними, але адаптивними, щоб команда могла коригувати дії залежно від унікальних обставин інциденту. Жорстко фіксований набір кроків не охопить усіх ситуацій, тому план має залишати простір для експертної оцінки та прийняття рішень у режимі реального часу.

По-третє – документування ролей та комунікацій окремо в плані фіксуються склад команди реагування і розподіл ролей: хто уповноважений приймати рішення, хто відповідає за технічні заходи, взаємодію з користувачами, зв’язок з керівництвом тощо. Чітке визначення відповідальності усуває плутанину під час кризової ситуації. Також план регламентує комунікації: встановлюються процедури оповіщення про інцидент (внутрішнього – керівництва, IT-підрозділів, співробітників, і за потреби зовнішнього – регуляторів, клієнтів, партнерів). Можуть бути підготовлені шаблони повідомлень для різних аудиторій (наприклад, внутрішнього сповіщення персоналу або публічного прес-релізу); проте детальні приклади комунікацій,

розглянуті раніше, тут не наводяться повторно. Основний акцент робиться на тому, що своєчасне інформування всіх зацікавлених сторін є критично важливим для обмеження наслідків інциденту та збереження довіри.

По-четверте – затвердження та впровадження після розробки основного змісту IR-плану документ проходить перевірку і затвердження керівництвом організації. Важливо переконатися, що план узгоджується з іншими внутрішніми політиками і регламентами. Затверджений план доводиться до відома всіх членів команди реагування та ключових менеджерів. На цьому етапі організація проводить навчання персоналу: відповідальні фахівці мають ознайомитися з процедурами, відпрацювати свої ролі та дії за планом. Впровадження плану включає також розповсюдження необхідних інструкцій і контактної інформації (наприклад, список екстрених контактів) серед команди. Таким чином, до моменту виникнення реального інциденту всі учасники процесу будуть готові діяти згідно узгодженого сценарію.

По-п’яте – тестування та вдосконалення ефективність плану реагування суттєво залежить від регулярного тестування і актуалізації. Після впровадження необхідно проводити тренування: наприклад, імітації інцидентів, навчальні «table-top» вправи чи технічні навчання для IT-фахівців. Такі тестові інциденти виявляють сильні та слабкі сторони плану. За результатами випробувань план коригується: уточнюються процедури, додаються нові сценарії, виправляються виявлені недоліки. Аналогічно, після кожного реального інциденту проводиться розбір польотів (етап *«Lessons Learned»*), щоб з’ясувати, що спрацювало, а що потребує покращення. Постійний цикл удосконалення гарантує, що IR-план залишається дієвим попри зміну обставин і появу нових кіберзагроз. Відповідно до провідних стандартів [1], процес реагування на інциденти носить циклічний характер: після завершення інциденту знання, отримані під час реагування, мають бути враховані при оновленні плану. Це підвищує готовність організації до майбутніх атак і забезпечує безперервне поліпшення системи безпеки. [4, 53].

У плані також слід передбачити класифікацію інцидентів за критичністю та відповідні сценарії реагування. Наприклад, інциденти рівня High (високий

пріоритет) – це такі, що спричиняють значний вплив на бізнес (витік даних клієнтів, зупинка критичних сервісів). Для них передбачений негайний збір команди, залучення керівництва і, можливо, повідомлення регулятора протягом 24 годин [7].

Практика показує, що наявність заздалегідь підготовлених шаблонів повідомлень (внутрішніх для співробітників, зовнішніх для клієнтів/партнерів, для прес-релізу) суттєво економить час у кризовий момент [54].

Варто також інтегрувати план реагування з планом забезпечення безперервності бізнесу та планом відновлення. Інциденти кібербезпеки часто впливають на безперервність бізнес-процесів, тому план реагування має бути узгоджений з планами резервного копіювання, відновлення після збою (Disaster Recovery) та іншими заходами забезпечення стійкості [53].

ENISA у своїх рекомендаціях наголошує: організація повинна мати “план Б” для швидкого відновлення критичних сервісів і зменшення середнього часу до відновлення (MTTR) [54].

Розробка і підтримка плану реагування на інциденти регулюється низкою галузевих стандартів та рекомендацій, які покликані уніфікувати підходи та забезпечити повноту охоплення всіх важливих аспектів. На міжнародному рівні одним із базових документів є NIST SP 800-61 (Computer Security Incident Handling Guide) від Національного інституту стандартів і технологій США. Він описує життєвий цикл реагування на інциденти і надає детальні настанови щодо підготовки IR-плану, формування команди, процесів виявлення, аналізу, стримування, відновлення тощо. Важливим принципом у керівництві NIST є акцент на безперервному вдосконаленні: після кожного інциденту організація повинна робити висновки і оновлювати свої процедури [15]. Таким чином забезпечується актуальність плану перед обличчям нових загроз.

Інші шаблони додають розділи про політики безпеки, глосарій термінів, список IT-активів, що підлягають захисту тощо.

Важливо, щоб план не був малозначним документом – він має бути реалістичним, зрозумілим для всіх учасників процесу та регулярно

оновлюватися.

Нерідко практикують затвердження плану на рівні керівництва компанії щорічно або після кожного суттєвого оновлення IT-ландшафту чи структури компанії [54]. Рекомендаційні етапи розробки плану реагування можна побачити в таблиці 3.3

Таблиця 3.3

Розробка плану реагування на інциденти

Етап розробки	**Конкретні завдання**	**Відповідальна особа**	**Термін виконання**
Виявлення інциденту	Реєстрація, класифікація інциденту	Аналітик безпеки	1 година
Первинна оцінка та ескалація	Встановлення рівня критичності, повідомлення відповідальних	Координатор реагування	2 години
Реагування та локалізація	Локалізація загрози, мінімізація наслідків	Головний інженер з безпеки	4 години
Усунення загроз і відновлення	Усунення загрози, відновлення систем	Адміністратор IT	8-24 години
Аналіз результатів та рекомендації	Аналіз ефективності, корегування плану	Менеджер з безпеки	Протягом 48 годин

Враховуючи динамічність кіберзагроз, переглядати і вдосконалювати план слід щонайменше раз на рік.

Отже, підготовка плану реагування на інциденти – це структурований процес, що включає визначення цілей, формування команди і ролей, документування покрокових процедур на всі фази інциденту, опрацювання різних сценаріїв та узгодження комунікацій. Грамотно складений і підтримуваний в актуальному стані план забезпечує “дорожню карту” дій у кризовій ситуації, що дозволяє зменшити хаос і невизначеність під час реального кіберінциденту. Етапи планування які рекомендовано для реагування на інциденти ІБ наведено в таблиці 3.4.

Таблиця 3.4

Етапи планування реагування на інциденти інформаційної безпеки

Етап	Зміст (основні завдання)
Підготовка вимог	Визначення нормативних вимог та бізнес-потреб; аналіз ризиків і можливих сценаріїв інцидентів.
Організація процесу	Призначення команди реагування та відповідальних осіб; розробка політики реагування на інциденти.
Розробка плану реагування	Створення детального плану дій для різних типів інцидентів; опис процедур виявлення, стримування, ліквідації та відновлення.
Затвердження та впровадження	Перевірка плану керівництвом, затвердження офіційно; доведення плану до співробітників, інтеграція у процеси організації.
Тестування та актуалізація	Проведення тестових вправ за планом (імітаційних інцидентів); виявлення та виправлення недоліків; періодичний перегляд і оновлення плану.

3.3 Проведення навчання персоналу щодо дій у разі інцидентів

Лише наявності плану реагування недостатньо – критично важливо, щоб відповідальний персонал був навчений і підготовлений діяти згідно з цим планом. Тренування і навчання підвищують готовність команди реагування, дозволяють відпрацювати взаємодію та “накачати м’язову пам’ять” для дій у стресовій ситуації. Існує декілька форматів навчання персоналу щодо реагування на інциденти, і ефективна програма зазвичай поєднує їх.

Перший рівень – теоретичне навчання: семінари, онлайн-курси, сертифікаційні програми. Співробітники вивчають основи процесу Incident Response, знайомляться з інструментами (SIEM, системами моніторингу, засобами форензики), засвоюють політики компанії. Наприклад, багато компаній використовують курси від SANS, EC-Council (Certified Incident Handler) чи внутрішні навчальні модулі на базі платформи LMS.[56] Також регулятори (той же NIST чи європейська ENISA) публікують відкриті методичні матеріали та навчальні посібники з реагування – їх можна адаптувати під свої потреби. Для широкого кола співробітників (не лише команди безпеки) проводяться курси підвищення обізнаності з кібербезпеки. ENISA вказує, що регулярний *awareness-*

тренінг для всіх співробітників є критично необхідним, бо багато інцидентів починаються з соціальної інженерії та фішингу.[57] Такі тренінги вчать розпізнавати ознаки кібератак та правильно діяти при підозрі на інцидент (наприклад, до кого звернутися, якщо отримано підозрілий лист).

Другий рівень – тренувальні сценарії на папері, або Tabletop Exercises (TTX). Це найпоширеніший формат навчання команди реагування. *Tabletop*-вправа являє собою модероторване обговорення умовного інциденту за заздалегідь підготованим сценарієм [58]. Учасники – члени CSIRT та дотичні менеджери – збираються разом (фізично або віртуально) і модератор поступово вводить обставини інциденту: наприклад, “Системні адміністратори помітили підозрілу активність на сервері баз даних…”. Команда повинна обговорити свої дії, хто що робить, які рішення приймаються. В ході дискусії модератор може додавати нові вводні (“з’ясовано, що витікли дані клієнтів”, “преса дізналася про інцидент” тощо), аби перевірити, як команда реагуватиме на розвиток ситуації. Такі вправи дозволяють виявити слабкі місця: чи всі знають свої ролі, чи зрозумілі процедури ескалації, чи не виникає плутанини у комунікаціях. Після завершення сценарію учасники разом з модератором проводять розбір: що спрацювало добре, а що потребує покращення. Рекомендації, отримані під час *tabletop*-сесій, потім використовуються для оновлення планів та інструкцій [59]. Прикладом *tabletop*-тренування може бути сценарій атаки віруса-шифрувальника на файловий сервер: команда в ході обговорення вирішує, чи відключати сервер, чи ізолювати мережу, як відновлювати дані з бекапів, як повідомити клієнтів про можливу недоступність сервісу тощо. В результаті такого навчання персонал набуває впевненості у своїх діях, а організація отримує цінну інформацію про готовність процесів.

Третій рівень – технічні симуляційні навчання. Вони вже ближчі до реальних умов, ніж *tabletop*. Наприклад, кібер-діапазони (Cyber Range) – це спеціальні віртуальні середовища, де імітуються IT-системи організації і запускаються навчальні кібератаки. Учасники (аналітики SOC, інженери безпеки) повинні в режимі, наближеному до реального часу, виявити атаку і

виконати дії реагування. Такі тренування дають змогу відточити технічні навички: роботу з консолями SIEM, аналіз трафіку, цифрову криміналістику, реагування засобами EDR тощо. Відомі приклади – навчальні програми від CISA, де учасники на кібер-полігоні проходять лаби з виявлення та розслідування APT-атаки на умовний фінансовий сектор [60]. Інший різновид – внутрішні симуляції інцидентів: коли команда безпеки свідомо генерує контрольований інцидент (наприклад, запускає тестовий зразок malware у сегменті мережі або проводить фішингову розсилку на співробітниках) і дивиться, як реагують процеси. Такі вправи ще називають *drills* (тренування на практиці). Вони можуть бути локальними (перевіряється окремий аспект, наприклад, чи спрацює оповіщення чергового інженера о 2 годині ночі) або більш комплексними [61].

Четвертий рівень – комплексні навчання на основі червоної команди (Red Team exercises). Формально це вже виходить за рамки чисто навчання персоналу і є повноцінним тестуванням безпеки (про що детальніше в підрозділі 3.4), але побічно також виконує навчальну функцію. Під час *red teaming* зовнішні або внутрішні фахівці діють як умовний “противник”, здійснюючи багатовекторну атаку на організацію, а синя команда (Blue Team) повинна цю атаку виявити та зупинити. Після завершення такої вправи обидві команди зустрічаються і обговорюють результати – цей формат часто називають фіолетова команда (Purple Team), коли нападники і захисники діляться знаннями [62]. Вигода для навчання персоналу колосальна: захисники на практиці бачать тактики і техніки реальних зловмисників, розуміють, які їхні дії були ефективними, а де вони пропустили атаку. Таким чином відбувається передача досвіду і підвищення кваліфікації через практику.

При виборі підходів до навчання слід враховувати ресурси і потреби організації. Невеликій компанії достатньо проводити періодичні *tabletop*-сесії і відправляти співробітників на зовнішні курси. Велика фінансова установа, яка є постійною мішенню для хакерів, зазвичай будує багатоетапну програму: щоквартальні *tabletop*-вправи для керівництва і IT, щорічні великі навчання за участі червоної команди, регулярні онлайн-курси для всіх працівників. У

банківському секторі також практикуються галузеві навчання. Наприклад, FS-ISAC організовує масштабні міжнародні кібер-вчення для фінансових компаній, де ті разом відпрацьовують реагування на інциденти і обмін інформацією. Це підвищує не лише готовність окремої установи, а й стійкість сектора в цілому.

Очікувані результати від навчання персоналу – це скорочення часу реакції (люди діють швидше і впевненіше, знаючи алгоритм), зменшення кількості помилок під час реальних інцидентів, налагоджена комунікація між підрозділами. Кінцевою метою є формування в організації культури, при якій кожен точно знає, що робити у разі кіберінциденту. Відзначено, що регулярні навчання значно підвищують ефективність всієї програми кібербезпеки: за даними IBM, компанії, які мають підготовлену команду та відпрацьовані плани реагування, економлять у середньому 1,5 млн доларів на вартості інцидентів порівняно з тими, хто не підготовлений. Це потужний аргумент на користь інвестування часу і ресурсів у тренування персоналу.

3.4 Проведення тестування реалізованих заходів реагування

Коли плани реагування розроблено і персонал навчено, наступним логічним кроком є випробування реалізованих заходів на практиці. Метою тестування є переконатися, що всі компоненти системи реагування – люди, процеси, технології – справді ефективно спрацьовують перед обличчям кібератаки. На відміну від планового навчання, яке може мати навчально-демонстраційний характер, тестування наближається до реального бою: імітуються загрози, і команда реагує так, ніби інцидент відбувається насправді. Це дозволяє виявити приховані недоліки, які не було помітно «на папері», і усунути їх до того, як трапиться справжня атака.

Рівні тестування. Практика показує, що ефективно використовувати кілька рівнів випробувань у комплексі. Перший рівень – локальні функціональні тести, які перевіряють окремі елементи процесу реагування. Наприклад, можна протестувати швидкість оповіщення: ініціювати умовний інцидент у неробочий

час і заміряти, за який час черговий інженер отримає повідомлення та приступить до дій.

Рівні тестування. Практика показує, що ефективно використовувати кілька рівнів випробувань у комплексі. Перший рівень – локальні функціональні тести, які перевіряють окремі елементи процесу реагування. Наприклад, можна протестувати швидкість оповіщення: ініціювати умовний інцидент у неробочий час і заміряти, за який час черговий інженер отримає повідомлення та приступить до дій

Інший приклад – drill з відновлення: відпрацювання процесу відновлення сервера з резервної копії, щоб з'ясувати, чи вкладаються IT-фахівці у заданий об'єкт відновлення (RTO) і чи не виникає технічних проблем при відновленні даних [17].

Другий рівень – технічні імітації атак (кібердрилі), про які згадувалося в підрозділі 2.3.

Тут організація вже перевіряє всю свою захисну інфраструктуру. Наприклад, у сегментів корпоративної мережі навмисно запускається контрольований зразок malware, і команда SOC відслідковує: чи спрацює антивірус і EDR, який сигнал надійде до SIEM, як черговий аналітик класифікує загрозу, які дії вживе для ізоляції зараженої машини. Або проводиться прихований *фішинг-тест*: розсилається навчальний фішинговий лист співробітникам і перевіряється, скільки людей піддались, чи помітить SOC аномальну активність і як відреагує на компрометацію обліковок.

Перевага таких тестів – вони наочно показують "профілактичну" ефективність засобів захисту та пильність персоналу. Якщо при симуляції атаки жодна система моніторингу не спрацювала, це тривожний сигнал: значить, у політиках виявлення є прогалини, які треба терміново виправляти. **Недоліком** є потенційний ризик: навіть тестова атака може спричинити збій або помилку, якщо, скажімо, malware вийде з-під контролю. Тому подібні випробування слід ретельно ізолювати від бойових середовищ і дотримуватися сценарію.

Третій рівень – повномасштабні командні вправи (*Red Team vs Blue Team*). По суті, це найскладніший вид тестування, який поєднує в собі елементи попередніх рівнів і додає фактор несподіванки.

Зовнішня або внутрішня команда *Red Team* діє абсолютно як справжній атакуючий(у межах узгодженого сценарію): використовує соціальну інженерію, проводить багатовекторні кібератаки, може спробувати фізично проникнути в офіс – тобто реалізує комплексну загрозу.

Blue Team, нічого не підозрюючи, повинна цю загрозу виявити та зупинити, керуючись наявними планами реагування. Важливо, що все відбувається в режимі, близькому до реального часу, без підказок і навчальних пауз.

Це випробування показує “в бою”, наскільки добре підготовлена організація: чи помітили атаку, як швидко ізолювали, чи змогли захистити критичні дані, як діяло керівництво (приймало рішення про відключення сервісів, комунікувало з зовнішніми стейкхолдерами).

Переваги тут максимальні – такий стрес-тест здатен виявити приховані слабкі місця у технологіях та процесах, про які ніхто не здогадувався.

З іншого боку, команда отримує неоціненний досвід: після завершення Red/Blue вправи проводиться детальний розбір (сесія *lessons learned*), де учасники обговорюють, що пройшло успішно, а де були помилки.

Наприклад, може з’ясуватися, що *red team* вдалось проникнути в мережу через давно незастосовуваний обліковий запис – отже, треба поліпшити політику управління обліковими записами; або що аналітики SOC пропустили атаку через завелике навантаження сигналами – значить, слід налаштувати фільтри і збільшити штат чи автоматизацію. Недоліки повномасштабних тестувань – це їхня складність, висока ціна і ресурсомісткість, а також неминучий стрес для персоналу Blue Team.

Проведення таких вправ вимагає зрілості: спершу організація має впровадити базові заходи і тренування, і лише досягнувши певного рівня готовності – випробувати себе “на міцність” через Red Team. Саме тому подібні тести зазвичай планують раз на рік або при зміні критичних систем. Результати впровадження тестувань можна побачити в таблиці 3.5.

Таблиця 3.5

Результати тестувань

Тип тестування	Дата проведення	Опис сценарію	Очікуваний результат	Фактичний результат	Виявлені проблеми	Рекомендації
Tabletop	10.04.2025	Симуляція фішинг-атаки	Швидке виявлення і блокування атаки	Виявлено за 30 хвилин, блокування через 1 годину	Недостатня швидкість блокування	Навчити персонал швидшому реагуванню
Red Team vs Blue Team	15.04.2025	Проникнення через слабкий пароль	Виявлення впродовж 15 хв	Виявлено через 45 хв	Вразливість через слабкі паролі	Зміна політики паролів, проведення навчань
Практична симуляція	20.04.2025	Атака ransomware	Локалізація атаки протягом 2 годин	Локалізовано за 3 години	Недостатньо швидка реакція команди	Вдосконалення процесів реагування

Також покращений час реагування та виявлення інциденту після кожного проведеного тестування відображено на рисунку 3.4.

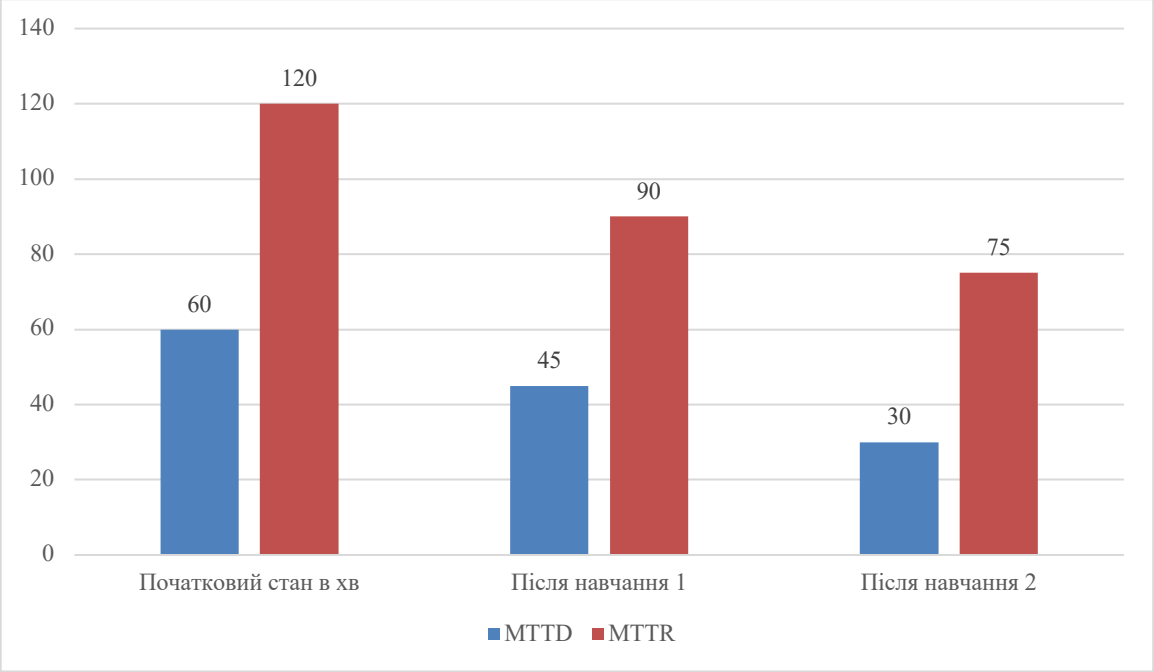

Рис. 3.4. Різниця часу реагування та виявлення до та після тестування

Реальні приклади та користь тестувань. На міжнародному рівні проводяться масштабні кібернавчання, що підтверджують ефективність комплексного тестування реагування. Приміром, у червні 2024 року відбулися загальноєвропейські навчання Cyber Europe 2024 під егідою ENISA [63], у яких узяли участь близько 5000 фахівців з різних країн. За підсумками цієї дводенної симуляції було зазначено, що навчання стало “цінним майданчиком для виявлення прогалин у поточних системах та процедурах і визначення напрямів для удосконалення” [64]. 92% учасників оцінили, що вправи значно підвищили їх рівень кіберготовності. Це яскраво демонструє: навіть дуже підготовлені команди знаходять слабкі місця під час комплексних тестувань і отримують можливість їх усунути у плановому порядку, а не під час реальних атак.

Інший приклад – аналітика компанії Mandiant. Їхні експерти зазначають, що попри зусилля з удосконалення захисту, *red team* при тестуванні здатна досягти ключової цілі (наприклад, отримати доступ до секретних даних) у середньому за 5–7 днів [35]. Це менше, ніж два робочі тижні, отже захисникам потрібно виявляти і нейтралізувати загрози ще швидше. Подібні результати тестувань мотивують організації вдосконалювати технології моніторингу та пришвидшувати процес реагування, аби не відставати від можливостей умовних “зловмисників”. Звіти IBM також підтверджують користь регулярних випробувань: середня шкода від інциденту істотно менша в тих компаній, які не лише мають план реагування, а й відпрацьовують його на практиці.

За даними IBM, у 2024 році різниця в середній вартості витоку даних між організаціями, які тестували свій план реагування, і тими, що цього не робили, складала сотні тисяч доларів [51]

Підсумовуючи результати таких випробувань, отримують цінний зворотний зв’язок: визначають, які процеси працюють бездоганно, а які потребують додаткового відпрацювання чи коригування. Важливо, що тестування заходів реагування – це не разова акція, а циклічний процес. Кожне випробування генерує цінний зворотний матеріал: що спрацювало добре, де були помилки, яких ресурсів забракло, чи всі учасники правильно зрозуміли свої ролі

тощо. У підсумку, організація підходить до реальних інцидентів уже загартованою: персонал діє злагоджено, знаючи свої задачі, технології налаштовані оптимально, плани перевірені практикою. Все це значно підвищує шанси вчасно зупинити атаку і зменшити її наслідки до мінімуму. У таблиці 3.6 наведено методи, особливості та заходи реагування на інциденти:

Таблиця 3.6

Класифікація методів тестування заходів реагування на інциденти

Метод тестування	Особливості та призначення
Документарний аналіз (аудит)	Перевірка наявності та якості документів реагування: політики, плани, процедури. Дозволяє виявити прогалини без практичного впливу на системи.
Імітаційне тестування (настільне)	Програвання сценаріїв інцидентів в режимі навчальних вправ (без втручання в роботу реальних систем). Дає змогу оцінити готовність команди та адекватність плану реагування.
Повномасштабне випробування	Практичне моделювання інциденту з залученням реальних систем (наприклад, контрольована кібератака або red team тест). Перевіряє ефективність усіх компонентів реагування в реальних умовах.

3.5 Оцінювання результатів практичної реалізації та формування рекомендацій

На завершення практичної реалізації заходів з підвищення готовності до інцидентів проводиться підсумкове оцінювання їх ефективності. Воно полягає у порівнянні ключових показників “до і після” впровадження заходів, аналізі динаміки змін та визначенні областей, що ще потребують вдосконалення.

За результатами, наведеними в попередніх розділах, організація досягла помітного прогресу. Зокрема, середній час виявлення (MTTD) скоротився з ~6 годин до ~4 годин, тобто на третину. Середній час реагування і відновлення (MTTR) зменшився приблизно з 20 до 12 годин, що майже на 40% швидше. Це означає, що потенційний “простій” бізнес-сервісів при кіберінцидентах тепер менший, а отже – менші збитки і ризики. Покриття сценаріїв інцидентів зросло з 60% до ~85%: після проведених навчань і оновлення планів організація опрацювала більшість критичних видів атак. Також збільшилась частота тренувань: замість двох разів на рік тепер тренування (різних форм) проводяться

щоквартально. Усі ці зміни – результат цілеспрямованих заходів планування, навчання та тестування.

Кількісну оцінку підкріплюють якісні спостереження. Команда реагування діє більш впевнено і проактивно, що відзначалося під час останніх навчань. Внутрішній аудит, проведений після реалізації заходів, показав позитивні зміни: політики та плани актуалізовані і закріплені наказом керівництва, інциденти документуються ретельніше, налагоджено процес уроків, винесених з кожного серйозного випадку. Звісно, залишаються і напрямки для покращення. Наприклад, аудит може зафіксувати, що хоча інциденти типу malware вже відпрацьовані добре, інциденти ланцюга поставок (supply chain) або атаки на хмарні сервіси поки що опрацьовані слабо – їх потрібно додати до програми тренувань. Або, що метрики MTTA (середній час підтвердження інциденту оператором) все ще зависокі у нічний час – можливо, варто запровадити цілодобове чергування більшеї кількості аналітиків чи вдосконалити систему оповіщення.

Корисно порівняти себе з галузевими бенчмарками. Наприклад, якщо глобальний медіанний час виявлення зараз ~10 днів (для складних атак), а в нашій організації він 4 години для відомих загроз – це дуже високий показник готовності. Якщо ж порівнювати з аналогічними компаніями у фінсекторі, де, припустимо, MTTD вимірюється годинами, а MTTR – менш ніж добою, то наші ~4 та ~12 годин відповідно є цілком конкурентними. Важливою є і економічна оцінка ефекту: згідно з дослідженнями, скорочення життєвого циклу інциденту на 61 день (за рахунок внутрішнього виявлення) економить майже $1 млн на один витік. У нашому випадку час до виявлення і реагування скоротився сумарно приблизно на 1–2 доби, що в масштабах потенційного інциденту теж може дати сотні тисяч доларів зекономлених втрат. Організація, яка інвестувала в підготовку, стала суттєво стійкішою: ймовірність успішної атаки або великих збитків знизилась. Це підтверджує тезу, що проактивні заходи безпеки є виправданими: за даними IBM, наявність команди реагування і планових тестів зменшує середню вартість інциденту на 15%.

На основі проведеного оцінювання формуються рекомендації для

подальшого вдосконалення. По-перше, рекомендується впровадити безперервний цикл покращення: переглядати план реагування щороку або після кожного значного інциденту, враховуючи уроки (Best Practices – *continuous improvement*). По-друге, варто розширювати використання автоматизованих засобів: наприклад, розглянути впровадження платформ SOAR (Security Orchestration, Automation and Response), щоб автоматично виконувати рутинні дії при інцидентах і ще більше скоротити MTTR. По-третє, продовжити практику регулярних навчань, залучаючи до них різні рівні персоналу. Зокрема, імітувати більш складні багатостадійні атаки (APT) і відпрацьовувати сценарії кризового управління для керівництва (кіберкриза, одночасний вплив на кілька підрозділів тощо). По-четверте, рекомендується посилити обмін інформацією із галузевими центрами (на кшталт CERT-UA, FS-ISAC): отримання свіжих *threat intelligence* та участь у спільних навчаннях допоможе підготуватися до новітніх технік атак, які з'являються. Також доцільно впровадити інструменти колективного обміну індикаторами компрометації (наприклад, платформу MISP) для швидкого збагачення даних про загрози і попередження інших учасників галузі.

Рис. 3.5. Порівняння ключових показників кіберготовності організації до і після впровадження заходів

Окремо аналізуючи приклад банку, можна надати такі рекомендації: продовжувати тренувати персонал з акцентом на реакцію на цільові атаки проти банків (шахрайство в платіжних системах, компрометація SWIFT тощо); провести *red team*–тест за методикою TIBER-EU (спеціальна програма етичного хакінгу для фінансових установ), що є найкращою практикою у європейських банках; інтегрувати в процес реагування сценарії кіберкриз – ситуацій, коли атака має системний характер і потребує взаємодії з держорганами та навіть правоохоронцями (для цього можуть стати в нагоді керівництва ENISA з кіберкризового менеджменту).

На завершення, підсумовуючи розділ: практична реалізація заходів з підготовки до інцидентів дала відчутний ефект – організація значно підвищила свою кіберстійкість, що підтверджено як метриками, так і успішним проходженням тестових ситуацій. Постійний розвиток і вдосконалення програми кібербезпеки має залишатися безперервним процесом. Середовище загроз еволюціонує, тому і готовність до реагування повинна перебувати на випередженні – через регулярне навчання, тестування нових підходів і коригування стратегії безпеки. Такий підхід забезпечить не лише ефективний захист від сучасних кіберінцидентів, але й створить основу для проактивного протистояння майбутнім загрозам. Порівняння ключових показників можна побачити у таблиці 3.7.

Таблиця 3.7

Порівняння ключових показників до та після впровадження підготовчих заходів

Показник	**До впровадження**	**Після впровадження**	
MTTD (середній час виявлення), год.	8 год	4 год	
MTTR (середній час реагування), год.		24 год	12 год
Покриття сценаріїв реагування, %		50 %	90 %
Частота навчань (кількість на рік)		1	4
Середні фінансові втрати на інцидент, тис. грн		800	200

Примітка: Дані умовні, але відображають реалістичну тенденцію покращення:

після впровадження заходів MTTD/MTTR знижуються, кількість навчань і покриття сценаріїв зростають, а середні втрати від інцидентів зменшуються (економія ~20% коштом швидшого реагування та меншого збитку). Цей графік наочно демонструє ефективність проведеної роботи та служить обґрунтуванням для керівництва щодо продовження інвестування в кібербезпеку.

Висновки до розділу 3

У розділі 3 реалізовано комплекс заходів, які суттєво підвищили готовність організації до реагування на кіберінциденти. Спочатку був проведений аудит і визначені ключові показники (MTTD, MTTR, покриття сценаріїв). На основі цього створено формалізований Incident Response Plan за стандартами ISO/IEC 27035 та NIST SP 800-61 з чіткими ролями та критичними сценаріями.

Кількісні результати підтвердили ефективність заходів:

a) MTTD скоротився з 6 до 4 годин (на 33%).

b) MTTR зменшився з 20 до 12 годин (на 40%).

c) Покриття сценаріїв зросло з 60% до 85%.

d) Частота тренувань зросла з 2 до 4 разів на рік.

Якісні зміни включають затвердження актуалізованих політик керівництвом, покращення документування інцидентів та впровадження процесу lessons learned після кожного серйозного випадку. Команда реагування стала діяти більш впевнено й злагоджено.

Залишаються напрями для подальшого покращення: наприклад, розробка сценаріїв реагування на атаки ланцюга поставок та хмарні сервіси, а також посилення нічних змін.

Отже, комплексні заходи значно підвищили рівень кіберзахищеності організації, забезпечивши швидше виявлення та ефективніше реагування, що знижує ризики і збитки від потенційних інцидентів.

ВИСНОВКИ

Виконане дослідження присвячено актуальній проблемі забезпечення готовності організацій до ефективного реагування на інциденти інформаційної безпеки. У роботі було системно розглянуто теоретичні засади та методичні підходи щодо організації процесів реагування, включаючи аналіз міжнародних стандартів і нормативних документів, які визначають сучасні практики у сфері кібербезпеки.

Під час дослідження було встановлено, що ефективність реагування значною мірою визначається рівнем підготовки персоналу та наявністю формалізованого плану реагування, який чітко регламентує ролі, відповідальності та послідовність дій під час інциденту. Особливу увагу було приділено аналізу методів навчання персоналу, серед яких важливими є теоретичні курси, практичні симуляції та комплексні командні тренування. Застосування таких методів у поєднанні з регулярним тестуванням планів реагування дозволяє суттєво скоротити час виявлення та локалізації кіберзагроз.

Практична реалізація розроблених заходів підтвердила їх ефективність. На прикладі умовно змодельованої фінансової організації було продемонстровано зниження середнього часу виявлення інцидентів на ~33% та підвищення рівня готовності персоналу приблизно 40%, завдяки системному навчанню та регулярному проведенню тренувань. Проведені тестування, включаючи penetration testing та навчання у форматі Red Team/Blue Team, дозволили виявити приховані вразливості та вдосконалити процедури реагування, що підтверджує важливість таких заходів для забезпечення кіберстійкості організацій.

У підсумку, виконана робота дозволяє стверджувати, що комплексний підхід, який включає ретельне планування, систематичне навчання персоналу та регулярне тестування заходів реагування, є критично важливим для ефективного управління ризиками інформаційної безпеки. Запропоновані у дослідженні рекомендації можуть бути використані в практиці підприємств для підвищення їх стійкості до сучасних кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Studfile.net. Preview 16435760. URL: https://studfile.net/preview/16435760/ (Дата звернення: 14.05.2025)

2. S-Byte.com. 27001.pdf URL: https://s-byte.com/useful/27001.pdf (Дата звернення: 14.05.2025)

3. Scribd.com. УІІС-Л5 URL: https://ru.scribd.com/document/825531293/УІІС-Л5. (Дата звернення: 14.05.2025)

4. NIST. Special Publication 800-61 Revision 2 URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf (Дата звернення: 14.05.2025)

5. Закон України “Про Національну поліцію” № 2163-19 URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Дата звернення: 14.05.2025)

6. LIGA:ZAKON. Текст договору TO001440 URL: https://ips.ligazakon.net/document/TO001440 (Дата звернення: 14.05.2025)

7. Національний банк України. Проект 04.11.2021 URL: https://bank.gov.ua/admin_uploads/article/proekt_2021-11-04.pdf (Дата звернення: 14.05.2025)

8. AMNafzar.net. ISO IEC 27035-1:2016 URL: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027035-1-2016.pdf (Дата звернення: 14.05.2025)

9. AMNafzar.net. ISO IEC 27035-2:2016 URL: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027035-2-2016.pdf (Дата звернення: 14.05.2025)

10. ISO.org. ISO/IEC 27035-3:2019 — Ed. 1 URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27035:-3:ed-1:v1:en (Дата звернення: 14.05.2025)

11. ArmorPoint.com. A Step-by-Step Guide to Incident Response: Practical Guidance from NIST SP 800-61. URL: https://armorpoint.com/2024/05/08/a-step-by-

step-guide-to-incident-response-practical-guidance-from-nist-sp-800-61/ (Дата звернення: 14.05.2025)

12. ENISA. Information Sharing and Analysis Centers. URL: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/information-sharing-and (Дата звернення: 14.05.2025)

13. FIRST.org. CSIRT Services, Roles and Competencies v 0.9.0 URL: https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Roles_and_Competencies_v_0.9.0.pdf. (Дата звернення: 14.05.2025)

14. FedRAMP. CSP Incident Communications Procedures URL: https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf. (Дата звернення: 14.05.2025)

15. NIST. SP 800-61 Revision 3 (Final) URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final. (Дата звернення: 14.05.2025)

16. TechTarget. Definition of SOAR. URL: https://www.techtarget.com/searchsecurity/definition/SOAR. (Дата звернення: 14.05.2025)

17. NetDiligence. Incident Response Plan Testing (2024). URL: https://netdiligence.com/blog/2024/10/incident-response-plan-testing/. (Дата звернення: 14.05.2025)

18. Juniper.net. What Is IDS/IPS? URL: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html. (Дата звернення: 14.05.2025)

19. Splunk.com. IT Event Correlation. URL: https://www.splunk.com/en_us/blog/learn/it-event-correlation.html. (Дата звернення: 14.05.2025)

20. NIST. NIST Special Publication 800-92 (Legacy) URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf. (Дата звернення: 14.05.2025)

21. PaloAltoNetworks.com. What Is SOAR? URL: http://www.paloaltonetworks.com/cyberpedia/what-is-soar. (Дата звернення: 14.05.2025)

22. Fortinet.com. WAF vs Firewall URL: http://www.fortinet.com/resources/cyberglossary/waf-vs-firewall. (Дата звернення: 14.05.2025)

23. PaloAltoNetworks.com. Difference Between WAFs and NGFWs. URL: http://www.paloaltonetworks.com/cyberpedia/difference-between-wafs-and-ngfws. (Дата звернення: 14.05.2025)

24. SANS.org. Incident Response Cycle (Form 504) URL: https://www.sans.org/media/score/504-incident-response-cycle.pdf. (Дата звернення: 14.05.2025)

25. Cynet.com. Incident Response SANS: The 6 Steps In-Depth. URL: www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/?utm_source. (Дата звернення: 14.05.2025)

26. BusinessWire. Mandiant M-Trends 2022 Report. URL: https://www.businesswire.com/news/home/20220419005242/en/Mandiant-M-Trends-2022-Report-Provides-Inside-Look-at-the-Evolving-Global-Cyber-Threat-Landscape-Directly-from-the-Frontlines. (Дата звернення: 14.05.2025)

27. NIST Glossary. Incident URL: https://csrc.nist.gov/glossary/term/incident. (Дата звернення: 14.05.2025)

28. Scribd.com. ISO-27035-1-2023 URL: https://ru.scribd.com/document/750725461/ISO-27035-1-2023?_gl=1*1warxst*_gcl_au*MzAzMTg0MjEyLjE3NDcwNzQ5NDU. (Дата звернення: 14.05.2025)

29. NIST. SP 800-61 Revision 3 URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r3.pdf. (Дата звернення: 14.05.2025)

30. ITSM-Docs.com. COBIT DSS02-01: Classification Schemes for Incidents and Service Requests. URL: https://www.itsm-docs.com/blogs/cobit-

framework/cobit-dss02-01-define-classification-schemes-for-incidents-and-service-requests. (Дата звернення: 14.05.2025)

31. Temple University MIS. COBIT 2019 Framework: Introduction and Methodology URL: https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf. (Дата звернення: 14.05.2025)

32. DXC.com. Why We Need More Cybersecurity Tabletop Exercises. URL: https://dxc.com/us/en/insights/perspectives/paper/why-we-need-more-cybersecurity-tabletop-exercises. (Дата звернення: 14.05.2025)

33. CloudShare.com. From Cybersecurity Training to Cyber Resilience: Benefits of Cyber-Range Platforms. URL: http://www.cloudshare.com/blog/from-cybersecurity-training-to-cyber-resilience-8-major-benefits-of-cyber-range-platforms. (Дата звернення: 14.05.2025)

34. Kroll.com. Why Conduct a Red Team Exercise? URL: http://www.kroll.com/en/insights/publications/cyber/why-conduct-a-red-team-exercise. (Дата звернення: 14.05.2025)

35. Google Cloud Blog. M-Trends 2024. URL: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024. (Дата звернення: 14.05.2025)

36. TechTarget. Average Cost of a Healthcare Data Breach URL: https://www.techtarget.com/healthtechsecurity/news/366599336/Average-cost-of-a-healthcare-data-breach-sits-at-977M. (Дата звернення: 14.05.2025)

37. RadiantSecurity.ai. AI Incident Response URL: https://radiantsecurity.ai/learn/ai-incident-response/. (Дата звернення: 14.05.2025)

38. BlinkOps.com. AI Incident Response URL: https://www.blinkops.com/blog/ai-incident-response. (Дата звернення: 14.05.2025)

39. AppGate.com. The Rising Costs of Data Breaches and the Role of AI [Електронний ресурс] URL: http://www.appgate.com/blog/the-rising-costs-of-data-breaches-and-the-role-of-ai-in-mitigating-risks. (Дата звернення: 14.05.2025)

40. Bank of England. CBEST Threat Intelligence-Led Assessments Implementation Guide. URL: https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide. (Дата звернення: 14.05.2025)

41. FFIEC. FFIEC Cybersecurity Assessment Tool (CAT) May 2017 URL: https://www.ffiec.gov/sites/default/files/media/resources/FFIEC_CAT_May_2017.pdf. (Дата звернення: 14.05.2025)

42. FFIEC. CAT Resources URL: https://www.ffiec.gov/resources/cat. (Дата звернення: 14.05.2025)

43. Table.media. Cost of a Data Breach Report 2024 URL: https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf. (Дата звернення: 14.05.2025)

44. SecurityScorecard.com. How to Use Incident Response Metrics [Електронний ресурс] URL: https://securityscorecard.com/blog/how-to-use-incident-response-metrics/. (Дата звернення: 14.05.2025)

45. UpGuard.com. Incident Response Plan URL: https://www.upguard.com/blog/incident-response-plan. (Дата звернення: 14.05.2025)

46. TechTarget. Red Team vs Blue Team vs Purple Team URL: https://www.techtarget.com/searchsecurity/tip/Red-team-vs-blue-team-vs-purple-team-Whats-the-difference. (Дата звернення: 14.05.2025)

47. UpGuard.com. Cost of Data Breach URL: https://www.upguard.com/blog/cost-of-data-breach. (Дата звернення: 14.05.2025)

48. Splunk.com. Mean Time to Detect (MTTD) URL: https://www.splunk.com/en_us/blog/learn/mean-time-to-detect-mttd.html. (Дата звернення: 14.05.2025)

49. Atlassian.com. Incident Management KPIs: Common Metrics URL: https://www.atlassian.com/incident-management/kpis/common-metrics. (Дата звернення: 14.05.2025)

50. Zscaler.com. 7 Key Takeaways from IBM’s Cost Data Breach Report 2024 URL: https://www.zscaler.com/blogs/product-insights/7-key-takeaways-ibm-s-cost-data-breach-report-2024. (Дата звернення: 14.05.2025)

51. IBM Think. Incident Response URL: https://www.ibm.com/think/topics/incident-response. (Дата звернення: 14.05.2025)

52. LinkedIn Advice. How Often Should You Conduct Incident Response Training? URL: https://www.linkedin.com/advice/0/how-often-should-you-conduct-incident-response-training-s9yle. (Дата звернення: 14.05.2025)

53. ENISA. Implementation Guidance on Security Measures (Public Consultation) URL: https://www.enisa.europa.eu/sites/default/files/2024-11/Implementation%20guidance%20on%20security%20measures_FOR%20PUBLIC%20CONSULTATION.pdf. (Дата звернення: 14.05.2025)

54. CISA. Incident Response Plan Basics URL: https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf. (Дата звернення: 14.05.2025)

55. ENISA. Best Practices for Cyber Crisis Management URL: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management. (Дата звернення: 14.05.2025)

56. SendPulse.ua. Learning Management System [Електронний ресурс] URL: https://sendpulse.ua/blog/learning-management-system. (Дата звернення: 14.05.2025)

57. ENISA. Awareness and Cyber Hygiene URL: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene. (Дата звернення: 14.05.2025)

58. RedCanary.com. How Do You Test an Incident Response Plan? URL: https://redcanary.com/cybersecurity-101/incident-response/how-do-you-test-an-incident-response-plan/. (Дата звернення: 14.05.2025)

59. CISA. Cybersecurity Tabletop Exercise Tips URL: https://www.cisa.gov/sites/default/files/publications/Cybersecurity-Tabletop-Exercise-Tips_508c.pdf. (Дата звернення: 14.05.2025)

60. CISA. Cyber Range Training Events URL: https://www.cisa.gov/resources-tools/training/cyber-range-training-events. (Дата звернення: 14.05.2025)

61. FS-ISAC. Exercises URL: https://www.fsisac.com/exercises. (Дата звернення: 14.05.2025)

62. Splunk.com. Purple Team URL: https://www.splunk.com/en_us/blog/learn/purple-team.html. (Дата звернення: 14.05.2025)

63. ENISA. Cyber Europe: Skills and Competences for Companies URL: https://www.enisa.europa.eu/topics/skills-and-competences-for-companies/cyber-europe. (Дата звернення: 14.05.2025)

64. ENISA. Cyber Europe AAR 2024 URL: https:/www.enisa.europa.eu/sites/default/files/2024-12/Cyber_Europe_AAR_2024_1.pdf. (Дата звернення: 14.05.2025)