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: “ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ ЧЕРЕЗ УПРАВЛІННЯ ІІБ”

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

_____ Антон ДОБРЕНЬКОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач(ка) вищої освіти гр. УБД-42

Антон ДОБРЕНЬКОВ
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна КАПЕЛЮШНА
Д.е.н., доцент Ім’я, ПРІЗВИЩЕ

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

Добренькову Антону Валерійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Забезпечення безперервності бізнесу через управління ІІБ”,

   керівник кваліфікаційної роботи КАПЕЛЮШНА Тетяна, д.е.н., доцент
   (ІПРІЗВИЩЕ, 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 2025 р.

3. Вихідні дані до кваліфікаційної роботи: *інциденти інформаційної безпеки, заходи стримування загроз, управління інцидентами, забезпечення безперервності бізнесу, нормативні документи, звіти з кібербезпеки, наукові публікації та практичний досвід компаній.*

4. Перелік питань, які мають бути розроблені:

   4.1. Проаналізувати природу інцидентів інформаційної безпеки та їх вплив на безперервність бізнес-процесів.
   4.2. Дослідити заходи стримування загроз інформаційної безпеки для забезпечення стабільної роботи підприємства.
   4.3. Вивчити підходи до управління інцидентами ІБ, оцінити ефективність реагування та сформувати рекомендації щодо підвищення кіберстійкості організації.

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 інцидентів інформаційної безпеки та їх впливу на безперервність бізнесу	08.04.2025	
4.	Дослідження заходів стримування інцидентів ІБ для забезпечення безперервності бізнесу	15.04.2025	
5.	Вивчення підходів до управління інцидентами інформаційної безпеки для підвищення кіберстійкості бізнесу	22.04.2025	
6.	Формування висновків щодо ефективності реагування на інциденти для забезпечення безперервності діяльності підприємства	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 ЕК.	__.06.2025	

Здобувач вищої освіти _____ Антон ДОБРЕНЬКОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(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 Добреньков А.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Забезпечення безперервності бізнесу через управління ІІБ"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачем ДОБРЕНЬКОВИМ Антоном у кваліфікаційній роботі обґрунтовано сутність ІІБ та проаналізовано їхній вплив на безперервність операційної діяльності; охарактеризовано існуючі заходи стримування загроз та здійснено критичну оцінку ефективності системи реагування на інциденти; проаналізовано недоліки чинної системи управління інцидентами, запропоновано комплекс рекомендацій щодо її удосконалення; проведено оцінку ефекту від запропонованих заходів із позицій безперервності бізнесу.

Бакалаврська кваліфікаційна робота відзначається актуальністю теми, оскільки дослідження торкається питань, що знаходиться на перетині управління інцидентами, інформаційної безпеки та безперервності бізнесу.

ДОБРЕНЬКОВ Антон продемонстрував здатність до системного мислення, володіння понятійним апаратом у галузі кібербезпеки, логічністю викладення результатів дослідження.

Означене вище дозволяє оцінити кваліфікаційну роботу здобувача - ДОБРЕНЬКОВА Антона на високу оцінку та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою «Управління інформаційною та кібернетичною безпекою».

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Добреньков А.В. 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 ДОБРЕНЬКОВА Антона
на тему: “Забезпечення безперервності бізнесу через управління ІІБ”

Інциденти інформаційної безпеки, які виникають внаслідок кібератак, технічних збоїв, зловмисної діяльності чи людських помилок, мають прямий вплив на стабільність функціонування підприємств, установ та організацій. Нерідко такі інциденти призводять до нестабільності функціонування бізнесу, втрати даних, фінансових збитків і репутаційних ризиків.

Дослідження, присвячене управлінню ІІБ й забезпеченню безперервності бізнесу, є практично значущим в умовах воєнного стану, ескалації кібератак на критичну інфраструктуру та необхідності забезпечення цифрової стійкості як на рівні підприємств, так і національної економіки в цілому.

Позитивні сторони.

1. Інтеграція завдань інформаційної безпеки з практиками управління безперервністю бізнесу (на перетині яких формується системний підхід) спрямована на мінімізацію негативного впливу кіберінцидентів, підвищення стійкості ІТ-інфраструктури, а також швидкість відновлення після критичних подій.

2. Представлені у роботі рекомендації, що спрямовані на забезпечення безперервності бізнесу через управління ІІБ.

Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

Недоліки.

Варто було б приділити увагу стандартизованим підходам до управління інформаційними інцидентами згідно з ISO/IEC 27035, NIST, що суттєво покращило б стійкість підприємств до кіберзагроз, а включення даного аспекту до переліку рекомендацій суттєво посилило б безпеку та забезпечило б безперервність функціонування бізнес-структур.

Однак дане зауваження негативно не відображається на загальному позитивному враженні про роботу та, відповідно, не впливає на позитивну оцінку кваліфікаційної роботи.

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

Рецензент: _____ Галина ГАЙДУР
д.т.н., професор, *підпис* Ім’я, ПРІЗВИЩЕ
завідувач кафедри Систем та технологій кібербезпеки

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню підходів до управління ІІБ для забезпечення безперервності бізнес-процесів підприємства. Робота складається зі вступу, трьох розділів, що містять рисунки, таблиці, висновки та список використаних джерел із 51 найменувань. Загальний обсяг становить 73 аркушів, з яких 7 аркуш займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження методів, процесів та технологій забезпечення безперервності бізнесу шляхом оперативного реагування на інциденти інформаційної безпеки.

Об'єкт дослідження – система управління інцидентами інформаційної безпеки на підприємстві як складова загальної системи захисту інформаційних активів.

Предмет дослідження – особливості застосування технологій управління ІІБ для зменшення негативного впливу на безперервність бізнесу.

Методи дослідження. У роботі використано методи аналізу, синтезу, класифікації, статистичного аналізу, експертного оцінювання та системного підходу. Також застосовано методи оцінювання ризиків для ідентифікації критичних загроз, які можуть порушити бізнес-процеси.

У процесі дослідження:

- проаналізовано природу інцидентів інформаційної безпеки та їхній вплив на бізнес-операції;
- систематизовано методи стримування та управління інцидентами для мінімізації збитків;
- вивчено ключові показники ефективності реагування (MTTD, MTTR, MTTC, тощо) та фактори, що впливають на їх покращення;
- наведено приклади з практики українських підприємств (ПриватБанк, Nova Post, Київстар) у протидії кібератакам;
- розроблено практичні рекомендації з побудови ефективної системи

управління інцидентами для забезпечення бізнес-стійкості.

Галузь застосування. Результати дослідження можуть бути використані при побудові систем управління інформаційною безпекою, підготовці планів реагування на інциденти (IRP), створенні команд CSIRT та впровадженні заходів забезпечення кіберстійкості в компаніях різних галузей.

Ключові слова: ІНЦИДЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ, УПРАВЛІННЯ ІНЦИДЕНТАМИ, СТРАТЕГІЯ РЕАГУВАННЯ, КІБЕРСТІЙКІСТЬ, MTTD, MTTR, IRP, CSIRT, РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ABSTRACT

The qualification thesis is dedicated to the study of approaches to information security incident management aimed at ensuring business continuity. The thesis consists of an introduction, three chapters containing figures and tables, conclusions, and a list of references comprising 51 sources. The total volume of the thesis is 73 pages, including 7 pages for the list of abbreviations and references.

The aim of the thesis is to examine the methods, processes, and technologies for ensuring business continuity through timely and effective response to information security incidents.

The object of the study is the information security incident management system within an enterprise as a component of the overall information asset protection system.

The subject of the study is the peculiarities of applying information security incident management technologies to mitigate the impact on business continuity.

Research methods. The thesis utilizes methods of analysis, synthesis, classification, statistical analysis, expert evaluation, and a systems approach. Additionally, risk assessment methods were applied to identify the most critical threats capable of disrupting business operations.

In the course of the research:

- the nature of information security incidents and their impact on business operations was analyzed;
- methods of incident containment and management were systematized to minimize damage;
- key performance indicators of incident response (MTTD, MTTR, MTTC, etc.) and the factors influencing their improvement were examined;
- real-world cases of Ukrainian enterprises (PrivatBank, Nova Post, Kyivstar) dealing with cyberattacks were reviewed;
- practical recommendations for building an effective incident management system to ensure business resilience were developed.

Scope of application. The results of this research can be applied to the

development of information security management systems, incident response planning (IRP), CSIRT team formation, and the implementation of cyber resilience measures in companies across various sectors.

Keywords: INFORMATION SECURITY INCIDENT, BUSINESS CONTINUITY, INCIDENT MANAGEMENT, RESPONSE STRATEGY, CYBER RESILIENCE, MTTD, MTTR, IRP, CSIRT, INFORMATION SECURITY RISKS.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ПЗ	Програмне забезпечення
СУБД	Система управління базами даних
СУІБ	Система управління інформаційною безпекою
ІІБ	Інцидент інформаційної безпеки

ВСТУП

Актуальність теми. Забезпечення безперервності бізнесу в умовах зростаючих кіберзагроз набуває особливої ваги. Сучасні підприємства дедалі більше залежать від цифрових технологій, і навіть один інцидент інформаційної безпеки(ІІБ) може спричинити значні перебої в роботі. Кількість кібератак постійно зростає, а їх наслідки стають усе серйознішими для організацій незалежно від розміру чи галузі діяльності. Паралельно зі збільшенням кількості атак зростають і фінансові втрати: витрати на ліквідацію наслідків інцидентів, відновлення інфраструктури та забезпечення нормального функціонування бізнес-процесів суттєво зростають.

Інформаційні інциденти можуть порушити цілісність та доступність критичних ресурсів, призвести до зупинки бізнес-процесів, втрати даних, зниження довіри клієнтів та репутаційних втрат. Це вимагає наявності ефективної системи управління ІІБ, яка дозволяє швидко реагувати на події, мінімізувати їх вплив та оперативно відновлювати діяльність. У зв’язку з цим дослідження механізмів управління ІІБ є вкрай актуальним, оскільки саме вони можуть забезпечити стабільність і безперервність бізнесу в умовах цифрових загроз.

Метою роботи полягає у дослідженні підходів до управління ІІБ з метою підвищення стійкості підприємства і забезпечення безперервності його бізнес-процесів.

Об’єкт дослідження – система управління ІІБ на підприємстві як складова загальної системи захисту інформаційних активів.

Предметом дослідження є методи, процеси та технології забезпечення безперервності бізнесу шляхом оперативного та ефективного реагування на ІІБ.

Завдання дослідження

- Проаналізувати природу ІІБ та їхній вплив на безперервність бізнес-процесів підприємства.

- Дослідити методи стримування та управління ІІБ, які дозволяють своєчасно локалізувати загрози і швидко відновити роботу систем.
- Вивчити показники ефективності реагування на інциденти (час виявлення, час відновлення, витрати на відновлення) та на цій основі сформувати практичні рекомендації щодо оптимізації цих показників.

Методи дослідження. У процесі виконання роботи було використано низку наукових методів, що забезпечили комплексний підхід до дослідження проблеми управління ІІБ. Зокрема, метод аналізу застосовувався для вивчення поточного стану проблеми та оцінки наявних рішень у сфері реагування на інциденти. Метод синтезу дозволив сформувати узагальнені підходи на основі опрацьованих матеріалів та практик. Системний підхід забезпечив цілісне бачення взаємозв'язків між компонентами системи управління інцидентами. Для дослідження реального впливу інцидентів використовувалися статистичні методи аналізу даних, що дозволило виявити ключові тенденції та закономірності. Аналітичне оцінювання для врахування досвіду фахівців у галузі кібербезпеки, а методи оцінювання ризиків — для виявлення найбільш критичних загроз, здатних негативно впливати на безперервність бізнесу.

Практичне значення одержаних результатів. На практиці значення роботи полягає у розробці рекомендацій та методичних підходів, які допоможуть підприємствам підвищити ефективність реагування на кіберзагрози. Запропоновані рішення дозволять зменшувати час простоїв інформаційних систем та мінімізувати фінансові втрати внаслідок ІІБ. Завдяки цьому організації зможуть зберігати працездатність критичних процесів навіть під час атак, що сприяє підтримці стабільності операцій і довіри клієнтів. Зокрема, формування кіберстійкості допоможе уникнути штрафних санкцій та юридичних витрат, пов'язаних з витоком даних, а також підвищить стійкість репутації компанії.

Апробація результатів. Результати дослідження були представлені на Всеукраїнській науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу», яка відбулася 27 лютого 2025 року.

РОЗДІЛ 1. ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЇХ СТРИМУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

1.1 Інциденти порушення інформаційної безпеки та безперервності бізнес-операцій

У сучасному цифровому середовищі навіть один скомпрометований електронний лист може призвести до низки проблем. Під ІІБ розуміють ситуацію, яка загрожує доступності, конфіденційності або цілісності даних. Однак на практиці це означає дещо більше наприклад вимушену зупинку роботи складу, паніку в контакт-центрі чи навіть замороження усіх банківських транзакцій через внутрішню компрометацію.

ІІБ – це подія або ряд небажаних чи неочікуваних подій, що становлять загрозу для конфіденційності, цілісності або доступності інформаційних активів організації. Такі інциденти можуть суттєво впливати на безперервність бізнес-операцій, спричиняючи простої в роботі, втрату даних, фінансові збитки та репутаційні втрати. Сучасні дослідження свідчать, що кіберінциденти стали однією з головних причин перебоїв у діяльності організацій по всьому світу. Згідно зі звітом IBM Security, глобальна середня вартість витоку даних у 2024 році досягла рекордних 4,88 млн дол. США[2]. Зростання цього показника пов’язане не лише з безпосередніми втратами даних, але й із все більш деструктивними наслідками інцидентів, які розширюють період простою і навантаження на ІТ-команди компаній. Наприклад, за останніми дослідженнями компанії Fastly, середній час повного відновлення після кіберінциденту у 2024 році становив 7,3 місяця, що на 25% довше, ніж очікувалося, і на місяць більше, ніж роком раніше. Для організацій, які скорочували витрати на кібербезпеку, ситуація ще гірша – вони фіксували в середньому 10,9 місяців на відновлення роботи після інцидентів[4]. Очевидно, що значні ІІБ можуть вивести бізнес-процеси з ладу на багато місяців, загрожуючи безперервності операцій та фінансовій стійкості бізнесу.

Наприклад, українська компанія «Укрзалізниця», яка працює у секторі логістики, у березні 2025 року стикнулась із зараженням онлайн-сервісів шкідливим ПЗ[1]. Упродовж декількох днів частина їхньої транспортної логістики була паралізована — значні черги на вокзалах, оскільки пасажири не могли придбати квитки через мобільний додаток або вебсайт. І це – не виняток. За даними IBM, середня глобальна вартість витоку даних у 2024 році перевищила 4,88 млн дол. США[2].

Інциденти, які раніше сприймались як малоймовірні, стали рутиною. За даними дослідження Arctic Wolf, майже половина опитаних компаній у 2023 році виявили ознаки хоча б одного успішного порушення безпеки [3]. І це ще не повна картина – багато з атак лишаються непоміченими, бо компанії не мають ані інструментів, ані кваліфікованих фахівців для їх виявлення, або просто не хочуть визнавати інциденти задля збереження свого іміджу. Таким чином, фактична частка бізнесів, що зазнали кібератак, ймовірно ще більша. Особливо небезпечними для безперервності бізнесу є цілеспрямовані атаки – зокрема рансомware-атаки, які шифрують дані чи блокують системи з метою вимагання викупу. Дослідження 2024 року показало, що 94% організацій, які постраждали від атак здирницького ПЗ, зазнали вимушених простоїв у роботі, причому 40% відчули повну зупинку бізнес-операцій на певний час [3]. Вартість простою та втраченої продуктивності часто перевищує навіть розмір викупу, що демонструє критичність цього виду інцидентів для бізнесу.

Наслідки масштабних інцидентів можуть обчислюватися сотнями мільйонів доларів та тижнями простою. Показовим є кейс глобальної атаки NotPetya (2017)[5], компанія Maersk, найбільший у світі контейнерний перевізник, внаслідок цієї кібератаки втратила доступ до своїх IT-систем на два тижні, що порушило роботу портових терміналів по всьому світу і змусило співробітників перейти на ручні резервні процеси. Фінансові збитки Maersk оцінила в 200–300 млн дол. США. Цей інцидент демонструє, що навіть високотехнологічні компанії можуть опинитися в ситуації повної зупинки бізнес-операцій.

Для розуміння природи ІІБ важливо врахувати їх різновиди. Існують різні підходи до класифікації ІІБ. В Україні впроваджено офіційний перелік категорій кіберінцидентів CERT-UA[6], розроблений на основі рекомендацій ENISA. Згідно з ним виділяють 10 основних категорій інцидентів, наведені в таблиці 1.1.

Таблиця 1.1

Класифікація ІІБ (CERT-UA/ENISA)

Категорія (код)	Опис та приклади
1. Шкідливий вміст	Поширення небажаного або протиправного контенту. *Приклад:* масова розсилка спаму, образливі матеріали.
2. Шкідливий програмний код	Інциденти, пов'язані зі зловмисним ПЗ (Malware). *Приклади:* зараження вірусом або трояном, розповсюдження шкідливого ПЗ, діяльність командно-контрольних серверів ботнету.
3. Збір інформації зловмисником	Розвідка та збір даних для підготовки атаки. *Приклади:* сканування мережі, перехоплення трафіку (*sniffing*), фішинг-атаки для викрадення даних.
4. Спроби втручання	Невдалі спроби порушення безпеки. *Приклади:* експлуатація вразливостей, численні неуспішні спроби входу (brute-force).
5.Втручання (компрометація)	Успішні проникнення в системи. *Приклади:* компрометація облікового запису користувача чи адміністратора; несанкціонований доступ до системи, отриманий через уразливість.
6. Порушення доступності	Атаки, що порушують нормальну роботу сервісів. *Приклади:* атака на відмову в обслуговуванні (DoS/DDoS), навмисний саботаж, а також непередбачений збій систем без зловмисного впливу.
7. Порушення цілісності інформації	Несанкціоновані дії з інформацією. *Приклади:* несанкціонований доступ до конфіденційних даних, їх модифікація або видалення.
8. Шахрайство	Кібер-шахрайство та зловживання ресурсами. *Приклад:* створення фішингового (шахрайського) сайту для викрадення даних користувачів.
9. Відомі вразливості	Наявність у системах відомих слабких місць. *Приклади:* незакрита відома уразливість, небезпечна конфігурація (налаштування за замовчуванням тощо).
10.Інше/Невизначені інциденти	Інциденти, що не підпадають під інші категорії або недостатньо даних для класифікації. Відносяться до типу "невизначений інцидент".

Виходячи з даних таблиці видно, що ІІБ охоплюють широкий спектр від спаму та вірусів до складних цільових атак і внутрішнього шахрайства. Кожен із

цих типів загроз по-різному впливає на бізнес-операції. Наприклад, DoS-атаки, безпосередньо зупиняють надання послуг клієнтам, інші(витоки даних) загрози можуть призвести до юридичних проблем та завдання шкоди репутації, що вдаряє по безперервності діяльності компанії. Спільним для всіх інцидентів є потенціал спричинити незапланований або неочікуваний простій і відволікти ресурси компанії, такі як гроші, або люди, на подолання наслідків замість виконання звичайних бізнес-завдань.

Особливо небезпечними для безперервності є інциденти, що поєднують кілька видів загроз. Наприклад, атака здирницького ПЗ може одночасно порушити доступність сервісів і спричинити несанкціоновану модифікацію/шифрування інформації, або включати елемент шахрайства при вимаганні викупу.

Такі комбіновані інциденти здатні повністю паралізувати бізнес-процеси. Згідно зі статистикою, бізнес-перерви, або зупинки, нині розглядаються як найдорожча складова кіберінцидентів. Дослідження страхових виплат за 2019–2023 рр. показало, що середні збитки від простою бізнесу внаслідок кібератаки для великої компанії склали 26 млн дол. США, тоді як загальна середня шкода від інциденту – 36 млн дол. США [7]. Отже, 72% витрат припадає саме на вимушений простій та пов’язані з ним втрати доходів. Для малого і середнього бізнесу різниця теж разюча. Інциденти без бізнес-перерв коштували в середньому ~ 205 тис. дол. США, тоді як із простоєм – майже 1 млн дол. США (із них ~ 487 тис. дол. США – власне втрачений дохід за час простою) [7]. Ці цифри підкреслюють, що операційна стійкість бізнесу прямо залежить від здатності організації протистояти інцидентам та швидко відновлюватися після них.

Таким чином, ІБ стали однією з головних загроз безперервності бізнес-операцій у цифрову епоху. Висока ймовірність їх виникнення, різноманітність векторів атак та значні наслідки (фінансові, репутаційні, правові) вимагають від організацій особливої уваги до питань готовності та реагування. Далі в підрозділах 1.2–1.3 буде розглянуто заходи стримування інцидентів та

організація управління ними для мінімізації впливу на бізнес-процеси.

1.2 Заходи стримування інцидентів-загроз для забезпечення безперервності бізнесу

Стримування інциденту (containment) – це фаза реагування, спрямована на те, щоб локалізувати загрозу і запобігти подальшому поширенню атаки в інфраструктурі. Фахівці порівнюють стримування з накладенням джгута при кровотечі – воно не “виліковує рану”, але не дає ситуації погіршитися, виграючи час для повного усунення проблеми [8]. У контексті безперервності бізнесу ефективне стримування – критично важливе, адже дає змогу звести до мінімуму каскадний розвиток інциденту, що міг би паралізувати операційну діяльність компанії. Як зазначається в огляді ReliaQuest, стримування є найвирішальнішою фазою реагування без якої навіть найкращі зусилля з виявлення та відновлення можуть зійти нанівець, дозволивши зловмисникам заглибити атаку та завдати ще більшої шкоди [9]. Іншими словами, швидке локалізування загрози визначає, чи залишиться атака “небільшою за інцидент” або ж переросте в повномасштабну кризу.

Для досягнення цієї мети застосовують термінові заходи короткострокового стримування, такі як відключення або ізоляція скомпрометованих хостів (від’єднання серверів, комп’ютерів чи інших пристроїв від мережі), блокування підозрілого трафіку на мережевому рівні (налаштування брандмауерів, відключення портів, сегментація мережі), тимчасове відключення уражених облікових записів чи привілеїв доступу тощо. Наприклад, негайне відключення заражених систем від корпоративної мережі та інтернету – перша рекомендація експертів при виявленні атаки. Цей крок не дозволяє шкідливому програмному коду або зловмиснику поширитися далі чи встановити зв’язок із зовнішніми командними центрами.

Важливо розуміти, що рішення щодо стримування часто потребують балансування між безпекою і доступністю сервісів. NIST радить заздалегідь

пропрацювати стратегії стримування для різних типів інцидентів та визначити допустимі ризики [10]. Якщо інцидент загрожує критично важливим системам, організація може піти на оперативне відключення деяких сервісів, аби зупинити “кровотечу” – навіть ціною короткострокового переривання бізнес-процесів. Такі рішення мають бути передбачені наперед у процедурах реагування. Як зазначено в NIST SP 800-61, рішення типу “відключити систему чи ні” значно легше приймати, коли існують наперед визначені процедури стримування, затверджені керівництвом. При виборі стратегії враховуються такі критерії, як потенційні збитки від продовження атаки, необхідність збереження доказів (щоб потім розслідувати інцидент), критичність сервісів (чи можна їх тимчасово зупинити), час і ресурси, потрібні на впровадження обраного заходу, а також тривалість дії рішення (тимчасове чи постійне). Наприклад, стримування DDoS-атаки вимагатиме зовсім інших дій (перенаправлення трафіку, фільтрація на рівні провайдера), ніж стримування вірусу-вимагача на окремому комп’ютері (ізоляція пристрою, активація резервних копій даних).

Одним з основних заходів стримування, що безпосередньо пов’язаний з безперервністю бізнесу, є активація резервних планів. Мова йде про переключення на резервні копії даних або дублюючі системи, якщо основні вражені. Наявність актуальних резервних копій критичної інформації в захищеному позамережевому сховищі дозволяє швидко відновити роботу навіть у разі успішної шифрувальної атаки[8]. Експерти наголошують на тому, що резервні копії слід регулярно тестувати і зберігати ізольовано, щоб вони самі не були заражені. У випадку атаки типу ransomware наявність чистих бекапів може бути рятівним колом для бізнесу – від їх наявності залежить, чи зможе компанія відновити операції без сплати викупу і скільки часу це займе. Ще один аспект – оперативна комунікація під час інциденту. Налагоджений канал зв’язку між командою реагування, IT-підрозділами та керівництвом допомагає швидко приймати рішення про стримувальні дії. В деяких ситуаціях також важливо сповістити бізнес-підрозділи про перехід на резервні процеси (наприклад, тимчасовий перехід на ручну обробку замовлень, якщо IT-система продажів

недоступна). Таким чином, заходи кібербезпеки мають узгоджуватися з планами Business Continuity – наприклад, відключення ураженого сервера повинно супроводжуватися запуском його резервного “дзеркала” чи перемиканням навантаження на альтернативний майданчик, якщо це передбачено планом безперервності.

Після реалізації невідкладних кроків із локалізації загрози (короткострокове стримування) необхідно переходити до довгострокових заходів стримування та ліквідації наслідків. До довгострокового стримування відносять більш ґрунтовні дії, спрямовані на те, щоб зловмисник не зміг відновити контроль над системою. Це може включати переконфігурацію сегментації мережі (щоб розділити і ізолювати вразливі ділянки), встановлення патчів для усунення уразливостей, через які стався інцидент, анулювання і перевипуск скомпрометованих облікових даних (паролів, сертифікатів) тощо[9]. Такі довгострокові заходи можуть займати від кількох годин до кількох діб, але вони необхідні, щоб забезпечити стабілізацію обстановки та підготувати ґрунт для повного відновлення систем. Зобразимо вищезазначене у вигляді таблиці 1.2

Таблиця 1.2

Заходи стримування інцидентів-загроз для забезпечення безперервності бізнесу

Інцидент	Наслідок (загроза безперервності бізнесу)	Заходи
Зараження системи шкідливим ПЗ	Ризик поширення загрози по мережі, паралізація операційної діяльності	Ізоляція заражених хостів, відключення від мережі, блокування трафіку, активація резервних копій
Несанкціонований доступ (компрометація облікового запису)	Можливість викрадення або знищення критичної інформації, зупинка сервісів	Відключення/блокування облікового запису, перевипуск облікових даних, оновлення політик доступу
DDoS-атака	Неможливість доступу до онлайн-сервісів	Фільтрація трафіку, перенаправлення через провайдера, зміна конфігурацій мережі
Ransomware-атака	Шифрування даних, зупинка роботи IT-систем	Ізоляція систем, відновлення з резервних копій, перевірка бекапів, анулювання зламаних облікових даних

Продовження таблиці 1.2

Інцидент	Наслідок (загроза безперервності бізнесу)	Заходи
Компрометація вразливої служби чи сервера	Поширення атаки на інші системи	Встановлення патчів, сегментація мережі, оновлення конфігурацій безпеки
Загальна кризова ситуація через кібератаку	Порушення критичних процесів, необхідність переходу на резервні сценарії	Активація резервних систем і процесів, ручна обробка замовлень, комунікація з бізнес-підрозділами

Варто підкреслити, що ефективне стримування безпосередньо знижує шкоду та час простою бізнесу. Досвід останніх років демонструє пряму залежність між швидкістю реагування і масштабом наслідків. Компанії, яким вдається ізолювати та зупинити атаку протягом перших годин, зазвичай уникають серйозних простоїв і швидше повертаються до нормальної роботи. Натомість затримка зі стримуванням дає змогу зловмисникам розвинути успіх – доексплуатувати інші уразливості, проникнути глибше в мережу, знищити чи викрасти більше даних.

Це підтверджується і статистикою, яка свідчить, що кращих практик відзначається тенденція до скорочення часу на стримування інцидентів. За даними SANS за 2023 рік, 76% кіберінцидентів вдавалося менше ніж за 24 години з моменту виявлення – це свідчить про велику увагу, яку організації приділяють оперативності реагування [11]. Водночас, якщо стримування провалене, наслідки можуть бути катастрофічними — окрім тривалого простою, організація стикається з зростаючими витратами на відновлення та ліквідацію шкоди. Сам IBM пов’язує зволікання з реагуванням із суттєвим подорожчанням інциденту, що й формує ті самі мільйонні збитки, про які йшлося вище. Тож заходи стримування — це своєрідний бар’єр, що відмежовує відносно керований інцидент від масштабної кризи, і міцність цього бар’єра визначає рівень безперервності бізнес-процнесів під час атаки.

На практиці до комплексу заходів стримування інцидентів слід віднести

такі кроки:

– Попередня підготовка та планування стримування. Організація ще до інциденту повинна розробити детальний план реагування на інциденти (Incident Response Plan), в якому прописані процедури стримування для різних сценаріїв атак. Наявність наперед визначених дій значно пришвидшує реакцію, адже команді не потрібно імпровізувати під час стресової ситуації[10]. План має визначати ролі і відповідальних осіб, канали комунікації, порядок відключення систем, критерії переходу на резервні потужності тощо.

– Технічні засоби швидкого реагування. Використання сучасних інструментів моніторингу та автоматичного захисту може саме по собі стримувати частину загроз в режимі реального часу. Наприклад, системи виявлення вторгнень (IDS/IPS) можуть автоматично блокувати підозрілу активність, рішення EDR (Endpoint Detection & Response) здатні ізолювати заражені кінцеві пристрої від мережі автоматично при виявленні шкідливого коду. Такі технології фактично реалізують аварійне стримування без втручання людини, що надзвичайно цінно, коли рахунок іде на хвилини. Згідно з дослідженнями IBM, впровадження засобів з елементами AI/Automation скорочує загальний час реагування більш ніж на 100 днів, а середню вартість інциденту – на 1,76 млн дол. США, що доводить ефективність технологічного підсилення фази стримування[12].

– Ізоляція та блокування. Як тільки інцидент підтверджено, першим кроком є ізоляція уражених компонентів: відключення серверів, робочих станцій або сегментів мережі, де помічено активність зловмисника. Одночасно, на мережевих пристроях блокуються відомі зловмисні IP-адреси чи домени, щоб розірвати зв’язок між внутрішньою мережею та зовнішнім атакувальником (особливо актуально при C2-комунікаціях ботнетів або вірусів). За необхідності – відключення інтернет-шлюзів для всієї компанії, якщо атака масштабна, аби запобігти виходу даних або розповсюдженню шкідливого коду далі.

– Збереження даних та журналів. Під час стримування важливо по можливості зберегти журнали та сліди атаки (файли дампів пам’яті, копії шкідливих файлів, логи систем), але пріоритетом є саме зупинка загрози. NIST застерігає від надмірного зволікання заради збору доказів – якщо дозволити атаці тривати, намагаючись “спостерігати” за зловмисником, це може дати йому час завдати ще більшої шкоди або використати скомпрометовану систему для атак на інших[10]. Тому баланс між стримуванням і слідством має вирішуватися на користь негайного припинення активної фази інциденту, особливо якщо йдеться про безперервність критичних сервісів.

– Активація резервних потужностей. У випадку, коли якийсь сегмент інфраструктури виведено з ладу або ізольовано, повинні запускатися процедури Disaster Recovery/Business Continuity: перемикання на резервний дата-центр, включення резервного серверу замість відключеного, використання резервних каналів зв’язку тощо. Це дозволяє підтримувати основні бізнес-функції, поки кіберінцидент ліквідовується. Наприклад, якщо основна база даних відключена через підозрілу активність, але існує її синхронна репліка на іншому майданчику, бізнес може продовжити роботу, підключившись до репліки, поки основна БД проходить очистку.

– Комунікація та оповіщення. Під час інциденту надзвичайної важливості набуває чітка комунікація: ІТ-служба сповіщає керівників бізнес-напрямів про масштаби проблеми, аби ті могли прийняти рішення (наприклад, тимчасово призупинити прийом замовлень на сайті, якщо стався витік даних і йде розслідування). За потреби активуються заздалегідь підготовлені плани кризових комунікацій – зокрема, якщо інцидент суттєвий, компанія може випустити публічне повідомлення чи оповістити клієнтів (це виходить за межі технічного стримування, але важливо для довготривалої бізнес-стійкості та репутації).

Рис.1.1 Комплекс заходів стримування інцидентів для забезпечення безперервності бізнесу

Отже, заходи стримування інцидентів – це комплекс дій, що дозволяють виграти час і простір для організації в умовах атаки. Ефективно локалізувавши загрозу, компанія може продовжувати надавати основні послуги (хай навіть в обмеженому режимі) та паралельно виконувати ліквідацію наслідків (eradication) і відновлення (recovery), про що йтиметься в наступному підрозділі. Головний принцип стримування – діяти швидко і рішуче, керуючись заздалегідь

продуманим планом. Це мінімізує шкоду, запобігає розвитку інциденту в кризу та захищає безперервність роботи бізнесу навіть під час інциденту.

1.3 Управління ІІБ для забезпечення безперервності бізнес-процесів (задачі, показники ефективності)

Управління ІІБ – це цілісний процес, який охоплює підготовку до потенційних інцидентів, їхнє виявлення, оперативне реагування (локалізацію і нейтралізацію загрози), відновлення постраждалих систем та аналіз отриманого досвіду. Метою такого процесу є мінімізація впливу інцидентів на бізнес-процеси та забезпечення їх безперервності навіть у разі атак чи збоїв. Багато провідних стандартів і методик зокрема NIST SP 800-61, ISO/IEC 27035 описують життєвий цикл реагування на інциденти, що зазвичай містить наступні основні фази[9]:

1. Підготовка (Preparation) – розробка політик безпеки, планів реагування, формування команди реагування на інциденти (CSIRT), навчання персоналу діям у кризових ситуаціях. На цьому етапі впроваджуються засоби моніторингу, проводяться тренувальні імітації інцидентів тощо. Якість підготовки багато в чому визначає успіх усіх подальших етапів.

2. Виявлення та аналіз (Detection and Analysis) – постійний моніторинг систем на предмет аномалій та ознак вторгнень, фільтрація та кореляція подій безпеки. При надходженні тривожних сигналів – їх аналіз, підтвердження факту інциденту, оцінка масштабів та потенційного впливу. В цій фазі важливо відрізнити справжні атаки від помилкових спрацювань. Швидке і точне виявлення є критичним: чим раніше виявлено проблему, тим більше шансів стримати її до мінімальних наслідків[13].

3. Стримування (Containment) – описаний детально в розділі 1.2 комплекс дій для локалізації інциденту та запобігання його ескалації. Стримування є своєрідним критичним пунктом: від його успішності залежить, наскільки обмеженими будуть збитки. Основне завдання – зупинити розвиток

атаки, вигравши час для повного усунення загрози.

4. Ліквідація (Eradication) – після локалізації переходять до повного знищення причин інциденту: видалення шкідливого коду, закриття вразливостей, відновлення скомпрометованих елементів системи до нормального стану. На цьому етапі, наприклад, проводиться чистка заражених машин, перевстановлення систем, заміна зламаних паролів, проведення форензики для знаходження “root cause” проблеми. Важливо переконатися, що усунуто всі сліди присутності зловмисника, інакше є ризик повторного зараження – тому нерідко перед ліквідацією здійснюють додаткову розвідку системи (сканування на бекдори тощо).

5. Відновлення (Recovery) – відновлення нормальної роботи всіх постраждалих сервісів і систем, повернення до штатного режиму функціонування. Сюди входить повернення ізольованих вузлів у мережу після переконання в їх безпечності, переведення навантаження назад на основні системи з резервних, ретельний моніторинг на випадок повторного появлення загрози. Фаза відновлення має забезпечити, що бізнес-процеси повністю працюють як до інциденту, а також що під час перехідного періоду (з моменту стримування до повного відновлення) вдалося дотриматися заданих бізнесом RTO/RPO (цільового часу відновлення і допустимої втрати даних).

6. Післяінцидентний аналіз (Lessons Learned) – завершальний, але надзвичайно важливий етап: аналіз дій до та під час інциденту, виявлення вдалих рішень і помилок, оновлення планів реагування та заходів захисту з урахуванням отриманого досвіду. Команда відповідає на питання: що спрацювало добре, що можна покращити, як запобігти такому інциденту в майбутньому. Цей процес безперервного вдосконалення підвищує кіберстійкість організації.

Кожна з перелічених фаз має на меті мінімізувати вплив інциденту на бізнес. Якщо процес управління інцидентами організовано належним чином, навіть серйозна кібератака не призводить до тривалих збоїв. Завдяки підготовці інцидент швидко виявляється, завдяки стримуванню він локалізується на ранньому етапі, ефективна ліквідація дозволяє усунути його без залишкових

“закладок” зловмисника, а злагоджене відновлення забезпечує швидке повернення бізнес-процесів до нормального стану. Таким чином, забезпечується безперервність або, принаймні, швидке відновлення безперервності бізнесу.

Узагальнено фази життєвого циклу реагування на інциденти представлено схематично на рисунку 1.2

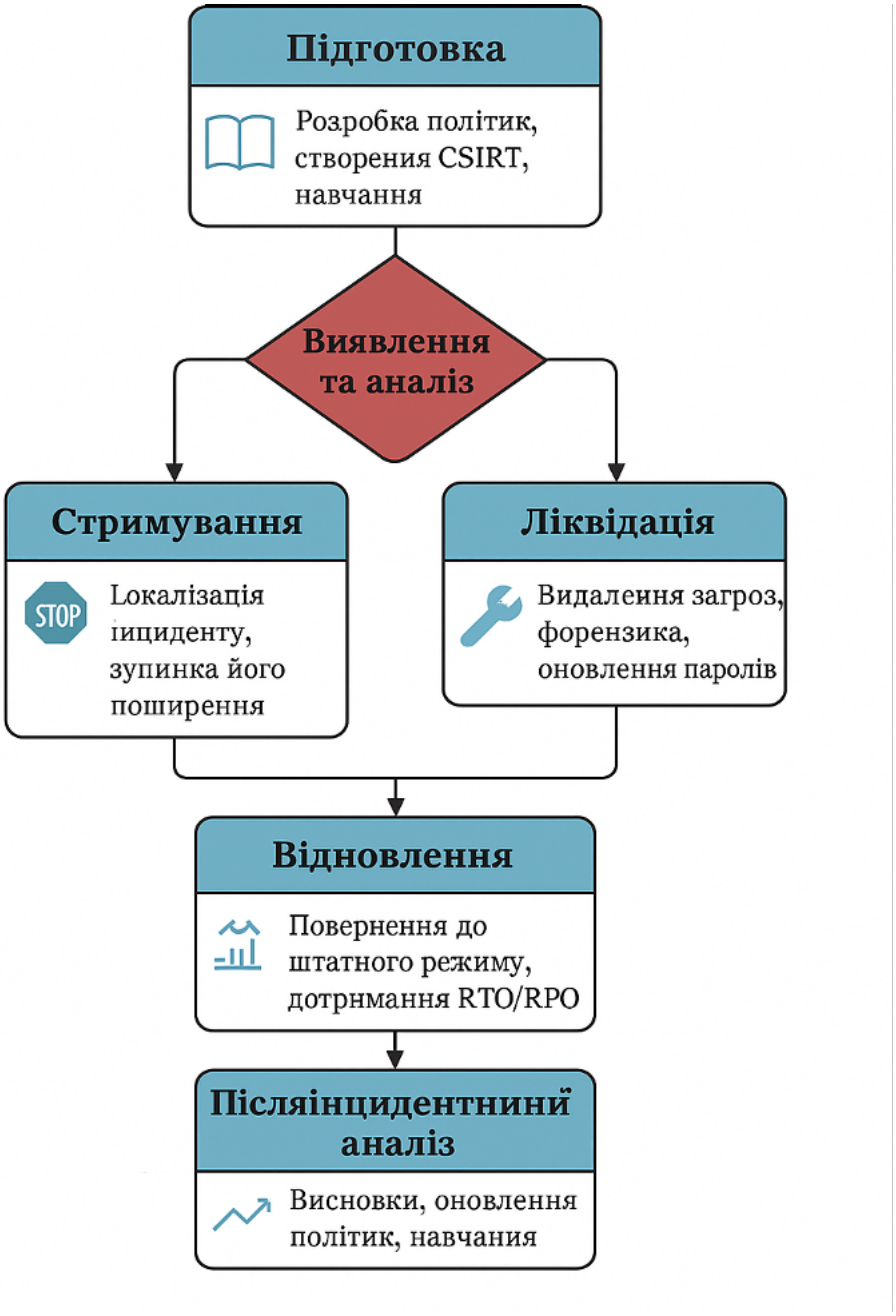

Рис. 1.2 Фази життєвого циклу реагування на інциденти

Для оцінки ефективності управління інцидентами в контексті забезпечення безперервності бізнесу використовують низку показників і метрик. Ці метрики

дають змогу виміряти, наскільки швидко і результативно організація реагує на інциденти, і виявити “вузькі місця” у процесах реагування. Нижче розглянемо ключові показники та фактори:

- Середній час виявлення (Mean Time To Detect, MTTD). Цей показник відображає, скільки в середньому часу минає від моменту фактичного виникнення інциденту до його першого виявлення командою безпеки або засобами моніторингу. MTTD є критично важливим: чим швидше компанія ідентифікує атаку, тим більше шансів обмежити її з мінімальними наслідками. Наприклад, якщо зловмисник отримав несанкціонований доступ, але був помічений за кілька хвилин, у нього менше можливостей наробити лиха, ніж у ситуації, коли проникнення залишалося непоміченим місяцями. За даними IBM, у 2023 році середній час виявлення+стримування становив 258 днів (приблизно 8,5 місяців) – найкращий показник за сім років, що свідчить про певний прогрес, але все одно багато інцидентів залишаються непоміченими надто довго. Вимірюючи MTTD, організації прагнуть зменшити його до годин або навіть хвилин[14].
- Середній час реагування/локалізації (Mean Time To Respond/Contain, MTTR/MTTC). Існують різні трактування MTTR: інколи мають на увазі Mean Time to Respond – час від моменту виявлення інциденту до завершення активних дій із його нейтралізації (локалізації та ліквідації загрози). Окремо виділяють Mean Time to Contain (MTTC) – середній час, необхідний, щоб ізолювати всі точки проникнення атаки і зупинити подальшу шкоду. Ці метрики показують, наскільки швидко команда може нейтралізувати загрозу після того, як її помітили. Наприклад, MTTC вимірює, скільки часу в середньому потрібно, щоб “зачинити всі двері” для зловмисника по всіх системах. Очевидно, чим коротший цей час – тим менше даних втратиться і тим скоріше системи будуть повернуті до роботи. Як зазначено в аналітиці, затягування інциденту прямо веде до зростання ризиків і витрат[13]. Тому компанії відстежують MTTR/MTTC і ставлять цілі знизити їх до мінімуму, впроваджуючи автоматизацію та покращуючи координацію дій.

- Середній час відновлення (Mean Time To Recover/Restore). Ця метрика більше стосується фази recovery – скільки в середньому часу займає повне відновлення роботи після інциденту (включно з перевірками і поверненням до нормального режиму). В контексті бізнесу її часто порівнюють із Recovery Time Objective (RTO), встановленою ціллю відновлення. Якщо середній фактичний час відновлення перевищує допустимий бізнесом RTO, значить процес реагування недостатньо ефективний з точки зору безперервності – слід шукати, де гальмує (наприклад, довго триває forensic аналіз чи перевірка даних). У згаданому вище дослідженні Fastly 2024 вказано, що очікуваний бізнесом час повного відновлення після інциденту – 5,9 місяців, але фактично виходить 7,3 місяця[4]. Завдання керування інцидентами – скоротити цей розрив.
- Кількість інцидентів за період та їх класифікація. Відстежується загальна кількість зареєстрованих інцидентів на місяць/квартал, а також їхній розподіл за категоріями та рівнями критичності. Це дозволяє оцінити, з яким навантаженням стикається команда реагування і які типи атак найчастіше загрожують безперервності роботи. Наприклад, якщо зростає частота ransomware-інцидентів (які критично впливають на доступність), то бізнесу варто інвестувати в додаткові заходи саме проти них (включаючи резервні системи). Крім того, метрика % інцидентів, що призвели до суттєвих перебоїв (скажімо, більше 1 години простою) теж показує ефективність: ідеально, якщо навіть більшість інцидентів не ескалують у значні порушення роботи завдяки своєчасному реагуванню.
- Процент інцидентів, виявлених внутрішніми засобами vs. зовнішніми. Цей показник показує, яка частка інцидентів була самостійно виявлена організацією (через SOC, моніторинг) проти тих, про які стало відомо від сторонніх (клієнтів, партнерів, правоохоронців тощо). Високий відсоток внутрішнього виявлення (близький до 100%) свідчить про зрілість систем моніторингу. За даними SANS, у ~47% організацій 75-100% інцидентів були виявлені внутрішньо, що відображає значний прогрес у можливостях

детектування[11]. Для безперервності бізнесу це важливо, адже зовнішнє виявлення зазвичай означає, що інцидент уже спричинив помітні наслідки (наприклад, клієнти повідомили про недоступність сервісу або витік даних став публічним). Тому мета – підвищувати власну проактивність.

- Показники успішності реагування. Сюди можна віднести частку інцидентів, успішно локалізованих до певного порогу часу (наприклад, % інцидентів, стриманих менш ніж за 4 години), частку інцидентів, що не переросли у витік даних або тривалий простій, і т.п. За опитуваннями, компанії демонструють поступове покращення: наприклад, протягом 2019–2023 рр. відсоток інцидентів, які локалізуються протягом першої доби, зріс на 17%[11]. Це прямий показник ефективності процесу реагування.
- Витрати на реагування на інциденти (сумарні та на інцидент). Хоч це бізнес-метрика, але вона теж відображає ефективність. Якщо інцидент ліквідовано “малою кров’ю” (мінімум залучених ресурсів, без понаднормових, без залучення дорогих консультантів) – значить процес налагоджений. Також сюди ж можна віднести штрафи за недотримання SLA чи регуляторних вимог через інциденти – їх відсутність свідчить, що інциденти не порушували критичних зобов’язань бізнесу.

Для успішного управління інцидентами важливо не лише відслідковувати метрики, а й розуміти фактори, що на ці метрики впливають. Дослідження та практика виділяють ряд факторів ефективності реагування на інциденти:

- Кваліфікація і підготовка команди. Наявність добре навченої, досвідченої команди реагування – один з найважливіших чинників. Добре підготовлена команда здатна реагувати швидко і злагоджено, що значно скорочує MTTD/MTTR[15]. Зворотній бік – кадровий голод: брак фахівців з кібербезпеки залишається глобальною проблемою. У 2024 р. опитані компанії назвали дефіцит кваліфікованого персоналу однією з найбільших перешкод для ефективного IR (incident response)[15]. Якщо в команді не вистачає людей або їм бракує навичок, інциденти будуть виявлятися пізніше і вирішуватися довше. Тому інвестиції в тренінги, сертифікацію, мотивацію і утримання

кадрів прямо впливають на показники реагування.

- Чіткі процеси і планування. Наявність формалізованого плану реагування, відпрацьованих процедур і сценаріїв (runbooks) допомагає уникнути хаосу при інциденті. Якщо процеси не визначені, час витрачається на з'ясування "що робити" замість власне дій. Половина організацій, за дослідженням Ponemon, зізналися, що у них відсутні значущі оперативні метрики для вимірювання ефективності реагування, а третина – що взагалі не має повноцінної команди CSIRT[16]. Це індикатор недостатньої процесної зрілості. З іншого боку, компанії, які регулярно тестують свій план реагування (наприклад, проводять навчальні кібервчення), досягають кращих результатів. IBM зазначає, що організації з пропрацьованою і протестованою процедурою IR економлять в середньому 1,49 млн дол. США на наслідках витоку даних у порівнянні з тими, хто не має відпрацьованого плану[12]. Тестування планів (table-top exercises, red team/blue team) виявляє слабкі місця до реального інциденту та підвищує готовність команди.

- Забезпеченість ресурсами та технологіями. Під "ресурсами" розуміються як інструменти (системи моніторингу, антивіруси, SIEM, засоби резервування, засоби автоматизації IR), так і фінансові ресурси (бюджет на реагування) і час, виділений співробітникам для цієї діяльності. Недостатнє фінансування було і залишається однією з головних проблем: навіть у 2024 р. обмежений бюджет названо в топі викликів, з якими стикаються команди ІБ. Якщо не вкладатися у сучасні засоби захисту, важко очікувати швидкого виявлення та стримування атак. Наприклад, аналіз мережевих audit trails (NetFlow, пакети) 80% фахівців назвали найефективнішим інструментом при розслідуванні інцидентів – але чи всі організації мають налаштований збір та аналіз таких даних[16]. Впровадження новітніх технологій (напр. систем з AI для детектування аномалій, SOAR-платформ для автоматизації реагування) може суттєво підвищити ефективність. З іншого боку, "зайві" технології без належної інтеграції теж не допоможуть – тому важлива правильна архітектура засобів безпеки. Додатково, до ресурсу відносяться і зовнішні партнери:

багато компаній залучають зовнішні послуги моніторингу та реагування (MDR, CERT-аутсорсинг). Тут теж баланс: якщо все віддано на аутсорс, внутрішня команда може втратити навички, але і тримати повністю in-house 24/7 SOC дорого. Опитування SANS показують, що інцидент-відповідь частіше лишають in-house, ніж моніторинг, через критичність і чутливість процесу[11].

- Культура та комунікації в організації. Ефективне реагування потребує злагодженої роботи не лише IT-відділу, а й всього бізнесу. Підтримка з боку керівництва забезпечує необхідні повноваження і ресурси для команди реагування. На жаль, дослідження свідчать, що топ-менеджмент часто мало залучений до питань кібербезпеки: лише 14% респондентів Ponemon в 2014 р. зазначили, що їх керівництво бере активну участь у процесі реагування[16]. Це ускладнює отримання ресурсів та прийняття швидких рішень під час кризи. Поступово ситуація змінюється з ростом усвідомлення кіберризиків. Так само, внутрішня культура – чи готові співробітники негайно повідомляти про підозрілі інциденти, чи проводяться після кожного інциденту “розбори польотів” без пошуку винних – усе це впливає на швидкість реакції. Налагоджені комунікаційні протоколи між IT-безпекою, IT-операціями і бізнесом запобігають непорозумінням під час атаки. Якщо ж між підрозділами “стіни” – реагування буксуватиме.

- Складність IT-ландшафту. Сучасні компанії мають розгалужені IT-системи: хмари, сотні застосунків, IoT, промислові системи тощо. Це розширює поверхню атаки і ускладнює реагування. За даними SANS 2023, все більше організацій відзначають виклик різнорідності та розподіленості інфраструктури (хмари, IoT, OT) як серйозний фактор, що ускладнює ефективний IR[11]. У таких умовах критично важливі інструменти централізованого огляду (EDR, лог-менеджмент), інакше інциденти можуть пройти повз радари. Також складність середовища може вимагати більшого часу на стримування (наприклад, важче ізолювати сегмент, коли він у хмарі з інтеграціями).

- Взаємодія з зовнішніми організаціями. Обмін інформацією про загрози (Threat Intelligence sharing) та співпраця з галузевими CERT може прискорити реагування (наприклад, отримавши IOC – індикатори компрометації – від партнерів, організація швидше виявить присутність атакуючого в своїй мережі). Проте майже половина організацій не ділиться інформацією про інциденти з іншими, що позбавляє їх колективного досвіду. Налагодження таких зв'язків– додатковий фактор підвищення готовності[16].

Згідно розглянутого матеріалу можна підсумувати як визначити кожну метрику та її нормальні значення, що буде зазначено наведені у таблиці 1.3

Таблиця 1.3

Показники оцінки ефективності управління інцидентами в контексті забезпечення безперервності бізнесу

Показник	Розрахунок(формула)	Норматив(допустиме значення)
Середній час виявлення (MTTD)	Σ(час виявлення кожного інциденту) / N	Менше 24 годин (оптимально — до 1 години)
Середній час реагування/локалізації (MTTR/MTTC)	Σ(час реагування кожного інциденту) / N	Менше 4 годин (оптимально — до 1 години)
Середній час відновлення (MTTRestore)	Σ(час повного відновлення) / N	Менше встановленого RTO (Recovery Time Objective)
Кількість інцидентів та їх класифікація	Підрахунок кількості інцидентів за період + категоризація	Низький рівень критичних інцидентів, стабільна динаміка
Процент внутрішнього виявлення інцидентів	(Кількість внутрішньо виявлених інцидентів / Загальна кількість) * 100%	Більше 75% (оптимально — близько 100%)
Частка успішно стриманих інцидентів	(Кількість стриманих інцидентів / Загальна кількість) * 100%	Більше 80% інцидентів стримано за 4 години
Витрати на реагування на інциденти	Σ(фінансові витрати на реагування за період) / N інцидентів	Мінімальні, без порушень SLA/регламентів

Підсумовуючи можемо зазначити, що ефективне управління інцидентами – це поєднання правильних процесів, людей, технологій і культури. Для підтримки безперервності бізнесу недостатньо лише купити засоби захисту; потрібно забезпечити, щоб вони швидко детектували загрози, команда чітко діяла за планом, мала потрібні навички і ресурси, а бізнес був готовий оперативно переключитися на резервні рішення. Регулярний моніторинг показників (часів реагування, тривалості простоїв, тощо) дозволяє кількісно оцінювати прогрес і аргументувати інвестиції в кібербезпеку на рівні керівництва. Зрілість процесу реагування напряму корелює зі зменшенням збитків. Як було показано, компанії, що впроваджують кращі практики (планування, автоматизація, тренування), суттєво скорочують як час простою, так і фінансові втрати від інцидентів. В умовах, коли кібератаки неминучі, швидкість та злагодженість реакції стають одним із визначальних факторів бізнес-стійкості.

Висновки до розділу 1

Інформаційна безпека тісно переплетена з безперервністю бізнесу адже сучасні компанії настільки залежать від інформаційних систем, що будь-який серйозний ІІБ може миттєво відбитися на їх діяльності. В цьому розділі проаналізовано природу таких інцидентів та підходи до їх стримування та управління заради мінімізації впливу на бізнес-процеси. Розглянуті дані з відкритих джерел демонструють, що кіберінциденти – одна з головних загроз безперервності від масових вірусних епідемій на кшталт NotPetya[5], що зупиняли цілі корпорації на тижні, до щоденних таргетованих атак здирників, які вимушено ставлять на паузу роботу багатьох організацій. Водночас, аналіз показує, що правильна підготовка і оперативне реагування здатні суттєво зменшити шкоду. Ключовими елементами наперед є продумані плани та класифікація інцидентів, що дозволяє не губитися в хаосі атаки, інструменти стримування (ізоляція систем, резервне відновлення) і ефективне управління процесом (тренована команда, чіткі метрики, постійне вдосконалення).

Одним з важливих результатів аналізу є усвідомлення, що інциденти неминучі, але катастрофічні наслідки – ні. Організації, які інвестують в кіберстійкість – наприклад, запроваджують регулярні навчання з реагування, автоматизують виявлення загроз, підтримують актуальні резервні копії – набагато краще переживають навіть важкі атаки. Як свідчить статистика, середній час реакції поступово знижується, а відсоток вчасно стриманих інцидентів зростає, що дає надію – бізнес починає випереджати зловмисників у здатності швидко оговтуватися від ударів. Водночас, виклики залишаються – зокрема, брак фахівців, складність ІТ-інфраструктури, еволюція самих загроз.

Для забезпечення безперервності бізнесу в умовах постійних кіберризиків компаніям варто розглядати інформаційну безпеку не як допоміжну ІТ-функцію, а як невід'ємну частину управління операційною стійкістю. ІІБ мають бути включені до сценаріїв планів неперервності (BCP), а команди реагування – тісно співпрацювати з командами управління кризами і відновлення. Тільки тоді, коли на всіх рівнях – від технічного до управлінського – буде досягнуто спільне розуміння загроз та відпрацьовано чіткі дії, організація зможе витримати серйозний кіберудар і продовжити роботу без значних втрат. Іншими словами, забезпечення безперервності бізнес-процесів сьогодні неможливе без зрілої системи реагування на ІІБ. Даний розділ заклав теоретичне і аналітичне підґрунтя цієї теми; в наступних розділах будуть розглянуті практичні аспекти побудови кіберстійкості та конкретні кейси протидії інцидентам.

РОЗДІЛ 2. АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ТА ЗАХОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

2.1 Особливості забезпечення інформаційної безпеки підприємства

У сучасних умовах підприємства мусять вибудовувати комплексну систему забезпечення ІБ, яка охоплює технологічні, організаційні та кадрові аспекти. Впроваджуються багаторівневі засоби захисту: політики безпеки, системи контролю доступу, шифрування даних, антивірусні та мережеві екрани, моніторинг та реагування на інциденти у реальному часі. Наприклад, ПриватБанк після кібератаки 2016 року суттєво посилив свою кіберінфраструктуру, інвестувавши у багатофакторну автентифікацію, цілодобовий моніторинг та вдосконалене шифрування для захисту даних клієнтів[17]. Крім того, банк впровадив програму Bug Bounty для залучення зовнішніх експертів до виявлення вразливостей: лише у 2023 році отримано 15 повідомлень про потенційні уразливості, 8 із яких були достатньо серйозними й одразу усунуті. Такий проактивний підхід демонструє, що великі компанії розглядають ІБ як стратегічний пріоритет і вкладають ресурси у її постійне вдосконалення.

Вагомою особливістю забезпечення ІБ є фізична та мережна сегментація інфраструктури, що мінімізує поширення загроз у разі інциденту. Провідні українські підприємства інтегрують резервні канали зв’язку та географічно рознесені центри обробки даних для стійкості до атак. Так, після масштабних кібератак останніх років (наприклад, вірусу Petya.A у 2017-му) багато компаній запровадили резервне копіювання та відмовостійкі хмарні рішення. Зокрема, логістична компанія «Нова пошта» (тепер Nova Post) була серед постраждалих від атаки NotPetya у червні 2017 року – діяльність відділень і контакт-центру тимчасово зупинялася[18]. Внаслідок цього підприємство прискорило цифрову трансформацію та міграцію критичних сервісів у захищені хмарні середовища, щоб забезпечити безперервність операцій навіть у разі компрометації окремих

ділянок. У 2023 році, під час військової агресії, Nova Post заявила про масштабне розширення IT-інфраструктури (проєкт Nova Digital) і впровадження рішень для захищеної віддаленої роботи та зберігання даних на хмарних платформах, що підвищує загальну стійкість систем.

Ще одним ключовим фактором є відповідність вимогам регуляторів та стандартів. Банківський сектор (ПриватБанк та ін.) дотримується норм НБУ щодо кіберзахисту, проходить регулярні аудити та сертифікації (наприклад, PCI DSS для платіжних систем). Телеком-оператори, такі як «Київстар», впроваджують політики ІБ згідно з рекомендаціями міжнародних стандартів (ISO/IEC 27001) та тісно співпрацюють з держрегулятором (Держспецзв'язку) для захисту критичної телеком-інфраструктури. Кадровий компонент теж є визначальним: створюються внутрішні підрозділи кібербезпеки (SOC – центри моніторингу безпеки), проводиться навчання персоналу з кібергігієни, розробляються плани реагування на інциденти. Наприклад, «Київстар» до атаки 2023 року мав команду ІБ, проте масштаб і новизна загрози виявили слабкі місця – зловмисники отримали доступ через зламаний акаунт підрядника[19]. Після цього випадку компанія анонсувала підсилення систем автентифікації контрагентів та додаткові тренінги для співробітників щодо виявлення ознак компрометації. Отже, забезпечення ІБ підприємства – це безперервний процес управління ризиками, що враховує специфіку галузі (банківська, поштово-логістична, телекомунікаційна) та динаміку актуальних загроз.

За статистичні даними Урядової команди реагування CERT-UA, у 2023 році в Україні було опрацьовано 2543 кіберінциденти, що на 15,9% більше, ніж у 2022 році. Найпоширенішими видами інцидентів були розповсюдження шкідливого програмного забезпечення (Malware), фішинг, зловмисні мережеві підключення, компрометація облікових записів та порушення цілісності систем[20]. Це узгоджується з глобальними тенденціями: за звітом IBM, середній глобальний збиток від витоку даних у 2024 році сягнув 4,88 млн дол. США, причому основними чинниками втрат стали простої в бізнесі та витрати на відновлення[21]. Висока частота шкідливих розсилок і атак соціальної інженерії

(фішинг) підтверджує необхідність посиленої уваги до людського фактора ІБ на підприємствах. Тому провідні українські компанії комбінують технічні рішення з просвітою персоналу, регулярними аудитами безпеки та тестуванням на проникнення, формуючи зрілу систему забезпечення ІБ, здатну протидіяти більшість типових атак.

2.2 Аналіз заходів стримування загроз ІБ підприємства

Стримування (containment) інциденту ІБ – критична фаза реагування, що має на меті локалізувати загрозу та запобігти її подальшому поширенню у системах підприємства. Ефективні заходи стримування дозволяють виграти час для відновлення і мінімізувати шкоду від атаки. Проаналізуємо, як принципи стримування реалізуються на практиці українських підприємств, зокрема на прикладах ПриватБанку, Nova Poshta та Київстар, які стикалися з реальними кіберінцидентами.

Однією з наймасштабніших атак на фінансовий сектор України стала DDoS-атака на ПриватБанк 15 лютого 2022 р. – вона вивела з ладу мобільний банкінг «Приват24» для клієнтів по всій країні. Стримування в цьому випадку полягало у швидкому фільтруванні шкідливого трафіку та перенаправленні його на «чорні дірки» (null-routing) за підтримки фахівців Держспецзв’язку і Нацполіції. Як повідомив Центр стратегічних комунікацій, фахівці оперативно «обрізали» основні напрями атаки, зокрема трафік з РФ та Китаю, а коли атака змінила географію – відбили і ці хвилі[21]. В результаті вже до кінця дня роботу основних веб-сервісів банку було відновлено. Такий кейс демонструє успішне стримування: атака тривала кілька годин і не спричинила втрати даних чи компрометації систем, обмежившись короткочасним збоєм окремого застосунку.

Інший характерний приклад – атака вірусу-шифрувальника Petya.A (NotPetya) у 2017 році, яка вразила ІТ-інфраструктуру багатьох українських компаній, в тому числі «Нова пошта»[18]. Коли 27 червня 2017 р. почалося масове зараження, ІТ-служба «Нової пошти» здійснила негайне стримування:

відключила робочі станції та сервери від мережі, щоб запобігти поширенню шкідливого коду, і призупинила обслуговування клієнтів. Попри вимушену паузу в роботі відділень, цей крок дозволив локалізувати проблему. Уже наступного дня компанія відновила роботу основних сервісів із резервних копій, фактично вигравши боротьбу з вірусом за рахунок швидкого ізолювання уражених систем[22]. Аналіз цього інциденту засвідчив дієвість заходів стримування: хоч бізнес-процеси тимчасово зупинились, вдалося уникнути довготривалого простою і втрати критичних даних. Отриманий досвід спонукав Nova Poshta переглянути стратегію реагування – зокрема, впровадити політику автоматичного відключення від корпоративної мережі комп'ютерів, на яких виявлено ознаки зараження, та регулярніше оновлювати резервні копії ключових баз даних.

Стримування загроз у сфері телекомунікацій має свою специфіку, що проявилось під час хакерської атаки на мережу «Київстар» у грудні 2023 року. Зловмисники проникли до IT-інфраструктури оператора та здійснили її цілеспрямоване руйнування[23]. Фактично, у перші години атаки (12 грудня 2023 р.) більшість систем контролю мережі було виведено з ладу, і мобільний зв'язок для 24 млн абонентів припинився. Команді реагування «Київстар» довелося застосувати стратегічне стримування: оператор відключив уражені сегменти мережі (зокрема, головний центр управління), щоб зупинити подальше «знищення» даних, та звернувся по допомогу до державних фахівців СБУ і Держспецзв'язку. Як наслідок, на час розслідування інциденту було тимчасово заблоковано національний роумінг для абонентів «Київстар», аби уникнути перевантаження мереж інших операторів та можливого поширення шкідливого впливу[24]. Хоча це рішення обмежило користувачів у можливості переключитися на резервний зв'язок, воно було вимушеним кроком для локалізації атаки. Лише ізолювавши зламані системи, фахівці змогли поступово відновити контроль: за тиждень основні послуги було відновлено, а за заявою президента компанії О. Комарова, кібератака зруйнувала близько 40% інфраструктури оператора. Таким чином, у випадку з «Київстар» стримування

набуло характеру масштабної операції з «відсічення» ураженої частини мережі, що хоч і спричинило значний простій, але не дало атакувальникам повністю знищити критичні вузли або проникнути в мережі інших операторів.

Загалом, заходи стримування загроз ІБ можна класифікувати за їх спрямованістю (Табл. 2.1). Відповідно до типу інциденту, підприємства застосовують різні комбінації дій:

Технічне стримування: відключення або ізоляція уражених серверів і сегментів мережі; блокування облікових записів, скомпрометованих під час атаки; активація систем виявлення і запобігання проникнень (IDS/IPS) у режимі блокування. Приклад: ізоляція поштових серверів Nova Poshta у 2023 р. після підозри на злам для запобігання витоку клієнтських даних.

Адміністративне стримування: тимчасове припинення певних бізнес-операцій або сервісів до локалізації загрози; переведення діяльності на резервні канали. Наприклад, «ПриватБанк» у випадку атак на державні реєстри в 2022–2024 рр. переходив на альтернативні джерела інформації для проведення клієнтських операцій, доки основні реєстри недоступні[25].

Комунікаційне стримування: оперативне сповіщення співробітників і клієнтів про інцидент та надання інструкцій щодо дій (щоб уникнути паніки й додаткових інцидентів, як-от фішинг на тлі основної атаки). Приклад: у ході DDoS-атаки 2022 р. ПриватБанк публічно запевнив, що загрози для коштів нема і проблеми суто технічні, чим попередив масові звернення клієнтів і зберіг довіру[21].

Спільне стримування із залученням держструктур: взаємодія з CERT-UA, Національною поліцією, СБУ для координації дій. Цей підхід був успішно застосований під час стримування атак на банківський сектор: робоча група основних суб’єктів кібербезпеки при Держспецзв’язку синхронно протидіяла DDoS, що дозволило відновити роботу банківських вебресурсів того ж дня[21].

Таблиця 2.1

Приклади заходів стримування кіберзагроз на підприємствах

Тип загрози	Заходи стримування	Приклад реалізації (кейс)
Зловмисний програмний код (Malware)	Відключення заражених пристроїв від мережі; ізоляція сегментів; оновлення антивірусних сигнатур, сканування систем	Nova Poshta, 2017: масове вимкнення систем під час Petya для запобігання поширенню вірусу.
DDoS-атака	Фільтрація трафіку на рівні мережевого провайдера; перемикання на резервні канали; динамічне блокування IP-адрес нападника	ПриватБанк, 2022: перенаправлення трафіку атакуючих на «чорну діру» за допомогою провайдерів і Держспецзв'язку.
Компрометація облікових даних	Примусове скидання паролів; блокування зламаних акаунтів; відключення скомпрометованих служб; додаткова автентифікація	Київстар, 2023: відключення доступу через зламаний обліковий запис підрядника, посилення контролю доступу після інциденту.
Витік конфіденційних даних	Відключення скомпрометованих баз даних; тимчасове призупинення інтеграцій з зовнішніми сервісами; аналіз журналів доступу; інформування клієнтів	(Гіпотетичний приклад) Виявивши несанкціонований доступ до БД клієнтів, Nova Poshta від'єднала БД від зовнішніх мереж та повідомила користувачів про зміну паролів.
Атака на IT-інфраструктуру (руйнівна)	Аварійне відключення критичних вузлів для запобігання фізичного знищення даних; активація резервних центрів обробки даних; залучення фахівців з кібербезпеки та правоохоронців	Київстар, 2023: відключення головного центру керування мережею, перехід на резервні сервери поетапно, залучення СБУ для нейтралізації атаки.

Анаілз даних вказує на різні типи атак, що, відповідно, потребують різних методів стримування, але спільною м:ою є обмеження масштабів інциденту. Ефективність стримування багато в чому залежить від наперед підготовлених планів реагування: компанії, що проводять таблиці зборів (tabletop exercises) та навчання персоналу діям у разі атаки, демонструють швидшу локалізацію загроз. Наприклад, за даними міжнародного досвіду, наявність відпрацьованого плану реагування дозволяє уникнути паніки та помилок у перші критичні години атаки, коли правильні кроки визначають подальший розвиток подій. Окрім того, своєчасне стримування інформаційних впливів (контроль комунікацій під час інциденту) допомагає запобігти вторинним загрозам. У випадку з атакою на

«Київстар», паралельно з технічними заходами, було важливо управляти інформаційним полем – офіційно підтвердити факт кібератаки та донести до громадськості необхідність часу для відновлення, що компанія й зробила того ж дня. Таким чином, стримування – це багатовимірний процес, який включає технології, організацію та комунікацію. Без ефективних дій на цьому етапі навіть найкращі системи захисту можуть зазнати поразки, адже атака, що не локалізована, здатна перерости у масштабну кризу.

2.3 Оцінка ефективності управління інцидентами

Ефективне управління ІІБ визначається здатністю організації вчасно виявляти, оперативно реагувати та мінімізувати наслідки інцидентів. Для оцінки результативності впроваджується система ключових показників (KPI), таких як середній час виявлення (Mean Time to Detect, MTTD), середній час реагування/ліквідації (Mean Time to Respond/Recover, MTTR), кількість інцидентів, оброблених за певний період, частка інцидентів, що призвели до простою тощо. Аналіз конкретних прикладів українських компаній дозволяє зробити висновки щодо успіхів і проблем у цій сфері.

Виявлення інцидентів – за глобальними дослідженнями, у 2024 році середній цикл життя кібервторгнення (від проникнення до повної ліквідації) становив близько 258 днів[26]. Це значення все ще вимірюється місяцями, хоча й дещо зменшилося порівняно з попередніми роками (277 днів у 2023). В Україні, з огляду на воєнний час, моніторинг кіберзагроз перебуває у посиленому режимі: CERT-UA повідомляє про виявлення тисяч підозрілих подій щодня[27]. Проте інцидент із «Київстаром» виявив недоліки саме на етапі детектування – як з’ясувала СБУ, хакери перебували в системі оператора з травня 2023 року, залишаючись непоміченими понад пів року. Це вказує на прогалини в засобах виявлення вторгнень (IDS/IPS) або нестачу кваліфікованого персоналу для аналізу сигналів. Подібні проблеми актуальні й для інших компаній: експерти відзначають, що майже половина бізнесів може не підозрювати про

скомпрометованість своїх систем. Водночас, позитивним прикладом є ПриватБанк, який звітує про успішне відбиття понад 1,16 млн атак лише за 2023 рік завдяки проактивному моніторингу та використанню AI-систем аналізу трафіку[17]. Це свідчить про високий рівень кібер-готовності: банк виявляє та блокує загрози ще на підступах, не допускаючи їх переростання у повноцінні інциденти. Отже, індикатором ефективності є співвідношення виявлених інцидентів до загальної кількості спроб атак – у ПриватБанку цей показник близький до 100%, тоді як у менш підготовлених організацій небезпечно багато атак проходять повз засоби детектування.

Швидкість та якість реагування – оперативність реагування вимірюється годинами й хвилинами, протягом яких команда ІБ ізолює та нейтралізує загрозу. Ефективне управління інцидентом передбачає, що після його виявлення чітко виконуються кроки згідно з планом реагування. В досвіді українських компаній можна побачити різницю в готовності до дій. ПриватБанк продемонстрував злагодженість під час DDoS-атаки 2022 року: служба ІБ і адміністратори за лічені години реалізували всі необхідні контрзаходи (від моніторингу до перенаправлення трафіку), і вже за ~5–6 годин система працювала стабільно[21]. Такий короткий MTTR (менше доби) свідчить про високий рівень підготовки і наявність наперед протестованого плану аварійного реагування. Nova Poshta у травні 2023 р. стикнулася із загадковим дводенним збоєм (який, за твердженням російських хакерів, був результатом їхньої атаки)[28]. Компанія не одразу визнала кіберінцидент, посилаючись на “технічні труднощі підрядника”, але водночас її фахівці за ~36 годин відновили роботу мобільного застосунку та поштоматів. Це вказує на певну ефективність реагування – швидке відновлення сервісів – проте недостатню прозорість комунікації. З іншого боку, кейс «Київстару» 2023 виявився найскладнішим: повне відновлення послуг зайняло 8 діб, а на розслідування та виправлення наслідків пішли тижні. Незважаючи на значні збитки, менеджмент компанії прийняв рішення компенсувати втрати клієнтам (скасування абонплати) та одразу подав позов до суду про незаконне втручання в роботу мережі. Це можна розглядати як елемент управління

інцидентом – робота з наслідками та юридичне реагування. Оцінюючи ефективність, слід врахувати безпрецедентний характер атаки на «Київстар»: зруйновано 40% мережевої інфраструктури [23], тобто компанія фактично проводила відновлення “з нуля” значної частини систем. Що важливо, її криза не перекинулася на суміжні сфери (банки, інші оператори), а це опосередковано свідчить, що реагування було координованим із загальнонаціональною системою кібербезпеки (ССОІ та СБУ). Такий координований підхід дозволяє знизити масштаб шкоди: напряму залучення правоохоронців та державних кіберфахівців зменшує збитки від інциденту на ~20%, прискорюючи технічне та слідче реагування[26].

Мінімізація впливу та відновлення – ефективність управління інцидентом остаточно визначається тим, наскільки швидко бізнес повернеться до штатної роботи і які втрати понесе. Успішне управління означає мінімальний простій і відсутність довгострокових наслідків (втрати даних, штрафів, репутації). Згідно з дослідженнями, наявність продуманого плану реагування і безперервності бізнесу може заощадити понад 1 млн дол. США потенційних збитків від одного інциденту[29]. Випадки ПриватБанку підтверджують цю тезу: банк зазнав кібератак різного типу (DDoS, спроби злому реєстрів, фішингові кампанії проти клієнтів), але завдяки підготовленості жодного разу не мав критичного збою, що вплинув би на фінансові показники або довіру вкладників. Компанія monobank (онлайн-банк), яку також атакували одночасно з ПриватБанком у 2022 році, відзвітувала, що хоча зазнала масованої DDoS-атаки, їй вдалося “тримати ситуацію під контролем” і уникнути простою. Це демонструє високий рівень операційної стійкості, коли інцидент не переходить у стадію бізнес-перерви. Натомість, ситуація з «Київстар» – приклад значного впливу: послуги зв’язку для мільйонів клієнтів були відсутні кілька днів, компанія понесла багатомільярдні збитки, а її конкурентам тим часом вдалося переманити частину абонентів[23]. Такий розвиток подій є ознакою того, що план забезпечення безперервності бізнесу (BCP) у випадку «Київстару» не зміг повністю компенсувати наслідки атаки. Ймовірно, підприємство не мало достатніх резервних потужностей для

швидкого перемикання трафіку або відмовостійких копій критичних систем. З іншого боку, варто відзначити здатність компанії відновитися протягом тижня навіть після настільки руйнівного інциденту – це стало можливим завдяки героїчним зусиллям її інженерів та допомозі партнерів (наприклад, колеги з Vodafone Україна надавали частину обладнання). Таким чином, міра ефективності тут двояка: з одного боку, упущення в підготовці призвели до тяжких наслідків, з іншого – кризове реагування дозволило уникнути повного колапсу бізнесу.

Для комплексної оцінки ефективності управління інцидентами доцільно розглянути фактори, що на неї впливають, що зазначено в таблиці 2.2. Досвід фахівців у сфері кібербезпеки та дослідження наковців дозволяють виокремити чинники, що посилюють спроможність організації протистояти інцидентам.

Таблиця 2.2

Фактори, що впливають на ефективність реагування на інциденти

Фактор	Вплив на ефективність реагування	Джерело / приклад
Наявність команди та плану реагування (IR Plan)	Чіткий розподіл ролей і напрацьовані процедури скорочують час ліквідації інциденту та знижують витрати. Організації з планом реагування заощаджують в середньому понад 1 млн дол. США на наслідках кожного інциденту.	IBM (глобальний звіт, 2024); ПриватБанк – регулярні навчання за планом дозволили уникнути хаосу під час DDoS-атак.
Регулярні навчання та кібервчення	Підготовлений персонал діє впевнено, що підвищує швидкість локалізації загрози. Табличні навчання (tabletop exercises) виявляють слабкі місця планів до реальних атак.	Держспецзв'язку у 2023 р. провела серію семінарів з реагування на інциденти для керівників критичної інфраструктури, що покращує загальнодержавну готовність[30].
Автоматизація моніторингу та виявлення (SIEM, SOC)	Системи на базі штучного інтелекту та кореляції подій швидше помічають аномалії, скорочуючи MTTD. Це зменшує масштаб атаки до стримування.	ПриватБанк запровадив AI для аналізу трафіку, що допомогло відбити понад 1 млн атак у 2023 р.
Залучення зовнішніх експертів (CERT, правоохоронці)	Координація з державними і галузевими CERT прискорює отримання розвідданих про загрозу та технічну підтримку. Взаємодія з правоохоронними органами може зупинити атакувальників та зменшити фінансові втрати (~–20% вартості інциденту).	Випадки банківських атак 2022 р.: спільна робота Нацполіції, СБУ та банків скоротила час відновлення сервісів.

Продовження таблиці 2.2

Фактор	Вплив на ефективність реагування	Джерело / приклад
Резервні системи та плани безперервності (BCP/DRP)	Наявність дублюючих серверів, резервних каналів зв'язку і актуальних бекапів дозволяє швидко перемкнутись на них, мінімізуючи простій.	Nova Poshta після атаки Petya відновила роботу з резервних копій менш ніж за добу. Відсутність належних резервів у «Київстар» призвела до тривалої перерви послуг.
Культура кібербезпеки та обізнаність персоналу	Якщо співробітники знають, як діяти при ознаках інциденту (неігнорувати дивні листи, повідомляти IT-службу тощо), інцидент може бути виявлено та локалізовано раніше, ніж спричинить шкоду.	За оцінками Verizon, людський фактор є головною причиною ~82% порушень ІБ; відтак, інвестиції в навчання напряму впливають на зниження частоти та масштабу інцидентів.

Як свідчать фактори в таблиці, проактивна підготовка (планування, навчання, резервування ресурсів) є визначальною для успішного подолання інцидентів. Українські підприємства, особливо в умовах війни, поступово підвищують свою кіберстійкість за цими напрямами. Наприклад, за 2022–2023 рр. кількість організацій, що мають власні команди реагування (CERT/SOC), значно зросла, а державні органи впровадили обов'язкове інцидент-сповіщення та обмін інформацією для критичної інфраструктури[31]. Це дозволяє не лише реагувати швидше в рамках окремого підприємства, але й запобігати ескалації інцидентів на національному рівні.

Важливо враховувати, що оцінка ефективності управління інцидентами – процес безперервний. Після кожного значного інциденту проводиться розбір польотів (post-incident review), який дає змогу виявити, що спрацювало добре, а де були недоліки. Культура вдосконалення на основі уроків інцидентів вже приживається в Україні: публічні заяви компаній про кібератаки тепер часто містять інформацію про кроки, яких буде вжито надалі. Так, після атаки на реєстри Мін'юсту у грудні 2024 р. банки повідомили про заходи, що впроваджуються для роботи в умовах відсутності держреєстрів[25]. Це свідчить

про зрілість підходу: інцидент розглядається не тільки як проблема, але і як мотивація для підвищення рівня безпеки.

Підсумовуючи, ефективність управління ІІБ найкраще проявляється у тому, що навіть за умови зростання кількості атак, бізнес-процеси підприємств залишаються безперервними або швидко відновлюються. Організації, які вкладають у превентивні заходи та розвиток компетенцій реагування, переносять кіберінциденти із розряду «надзвичайних ситуацій» до рівня керованих операційних ризиків.

Висновки до розділу 2

У розділі 2 проведено аналіз практичних аспектів забезпечення ІБ підприємства та заходів безперервності бізнесу на прикладі трьох провідних українських компаній – ПриватБанку, Nova Poshta та Київстар. Дослідження показало, що:

Ефективний захист підприємства досягається багаторівневим підходо, тобто комплексністю системи ІБ, якиа поєднує сучасні технологічні рішення (мережевий захист, моніторинг, шифрування, резервування) з організаційними заходами (політики, процедури, навчання персоналу). Особливістю останніх років стало посилення уваги до кібербезпеки в умовах війни: компанії інвестують у стійкість інфраструктури, розносять ресурси географічно, співпрацюють із державними органами задля своєчасного отримання інформації про загрози. Приклад ПриватБанку демонструє високу ефективність проактивних дій – впровадження нових технологій (AI для моніторингу, Bug Bounty) та міжнародних стандартів дозволило банку успішно відбивати численні атаки без переривання бізнес-операцій.

Аналіз кейсів підтвердив ключову роль фази стримування у мінімізації шкоди від атак. Вчасне локалізування загрози (відключення уражених систем, блокування атакувального трафіку, ізоляція) неодноразово убезпечило українські компанії від катастрофічних наслідків. Зокрема, стримування DDoS-атак на банки у 2022 році та вірусу Petya.A у Nova Poshta у 2017 році дозволило

уникнути тривалих простоїв і зберегти цілісність даних. Водночас досвід атаки на «Київстар» показав, що відсутність негайного стримування (через пізнє виявлення) призводить до значно більших руйнувань інфраструктури. Отже, підприємствам критично необхідно мати наперед відпрацьовані сценарії стримування для різних типів інцидентів, а також забезпечити ресурси для їх реалізації (резервні канали, фахівці на чергуванні, контакти з CERT тощо).

Ефективність управління інцидентами оцінюється здатністю організації швидко відновити роботу і мінімізувати втрати. В досліджених прикладах ми побачили широкий спектр результатів: від майже непомітних для клієнтів збоїв (ПриватБанк, monobank під час DDoS) до масштабних криз (тижневий простій «Київстару»). Фактори, що зумовлюють таку різницю, включають рівень підготовленості (наявність команди реагування, планів BCP/DRP), технологічну оснащеність (системи раннього виявлення, резервні потужності) та взаємодію із зовнішніми структурами. Підприємства, що заздалегідь подбали про ці аспекти, продемонстрували значно кращі показники реагування (нижчі MTTD/MTTR, менший вплив на клієнтів). Важливо, що інвестиції у підготовку окуповуються: за даними міжнародної аналітики, налагоджене управління інцидентами економить суттєві кошти, зменшуючи прямі збитки і штрафи та запобігаючи втраті довіри клієнтів.

Зростання кількості кіберінцидентів є стійкою тенденцією (CERT-UA фіксує +15–62% інцидентів на рік), отже питання ІБ та безперервності бізнесу набувають ще більшої актуальності. Найпоширеніші атаки (шкідливий код, фішинг, DDoS) відносно добре відомі і типові заходи протидії їм відпрацьовані на практиці українських підприємств. Однак з’являються нові виклики – комбіновані та цілеспрямовані атаки (як-от випадок з «Київстар», що поєднав елементи внутрішньої компрометації і саботажу мережі). Це вимагає підвищення рівня кіберготовності до найгірших сценаріїв, включаючи підготовку до роботи в режимі надзвичайної ситуації.

Загалом, аналіз показав, що забезпечення ІБ підприємства та безперервності його бізнес-процесів – це комплексне завдання, яке потребує

системного підходу та постійного вдосконалення. На прикладі ПриватБанку, Nova Poshta та Київстар було продемонстровано важливість інвестицій у кіберстійкість, швидкого стримування інцидентів та ефективного реагування. Отримані уроки підтверджують: чим вищий рівень зрілості системи управління інцидентами, тим меншою є вразливість бізнесу до сучасних кіберзагроз, а отже – тим надійніше забезпечується безперервність його діяльності в цифрову еру.

РОЗДІЛ 3. УПРАВЛІННЯ ІНЦИДЕНТАМИ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

3.1 Недоліки в управлінні ІІБ та їх вплив на безперервність бізнесу

У сучасних умовах кіберзагроз якісне управління ІІБ (ІБ) є критичним для безперервності бізнесу. Проте на практиці існує низка недоліків у процесах реагування на інциденти, які знижують ефективність захисту і можуть призвести до тривалих простоїв та збитків для організацій. Для розуміння проблем варто спершу навести класифікацію можливих інцидентів. В Україні впроваджено єдину таксономію кіберінцидентів, затверджену Національним координаційним центром кібербезпеки. Згідно з цією таксономією, усі ІІБ поділяються на 10 категорій (табл. 3.1), що охоплюють від шкідливого контенту до порушення доступності та шахрайства.[32]

Таблиця 3.1

Перелік категорій ІІБ (CERT-UA/NKCK)

Код	Категорія інциденту (укр / англ)	Приклад
1	Шкідливий вміст (*Abusive Content*)	Розсилка спаму, компроментуючі матеріали в мережі.
2	Шкідливий програмний код (*Malicious Code*)	Зараження вірусом, виявлення шпигунського ПЗ.
3	Збір інформації зловмисником (*Information Gathering*)	Сканування портів, перехоплення трафіку (sniffing).
4	Спроби втручання (*Intrusion Attempts*)	Спроби експлуатації вразливостей систем.
5	Втручання (*Intrusion*)	Успішний злом облікового запису або системи.
6	Порушення доступності (*Availability*)	Атака типу DoS/DDoS, саботаж обладнання.
7	Порушення властивостей інформації (*Information Content Security*)	Несанкціонований доступ до конфіденційних даних, модифікація інформації.

Продовження таблиці 3.1

Код	Категорія інциденту (укр / англ)	Приклад
8	Шахрайство (*Fraud*)	Фішинговий вебсайт, фінансові шахрайські операції.
9	Відома вразливість (*Vulnerable*)	Виявлення критичної вразливості або некоректної конфігурації.
10	Інше (*Other*)	Інцидент, що не підпадає під зазначені категорії.

Як показано в таблиці 3.1, інциденти бувають різного характеру – від кіберхуліганства (спам чи образливий контент) до критичних збоїв (відмова сервісів, компрометація систем). Управління інцидентами передбачає своєчасне виявлення, аналіз, стримування та відновлення після будь-якого з таких інцидентів. Однак досвід останніх років і аналітичні звіти вказують на типові проблеми в організації цього процесу. Нижче розглянуто основні недоліки у реагуванні на ІІБ та їхній вплив на бізнес-процеси компанії.

Однією з головних проблем є невизначеність процедури дій при інцидентах і ролей учасників. Багато компаній все ще не мають формалізованого плану реагування на інциденти (IRP – *Incident Response Plan*). Згідно з дослідженням Ponemon Institute 2023 року, 77% опитаних організацій визнали, що не мають формалізованого плану реагування на кіберінциденти[33]. Відсутність чіткого плану призводить до імпровізації під час атаки: персонал не знає, хто саме за що відповідає, які кроки слід виконати насамперед. В результаті цінні години можуть бути втрачені через плутанину та хаотичні дії. Як наслідок, затримується локалізація та ліквідація загрози, збільшується тривалість простою ІТ-систем. Дослідження підтверджують, що без стандартизованого процесу реагування інциденти вирішуються значно повільніше і з вищими втратами. Таким чином, відсутність планування прямо підриває безперервність бізнесу, оскільки компанія не готова оперативно повернутись до нормальної роботи після події.

Наступний критичний недолік – брак фахівців з кібербезпеки або виділеної команди реагування. Навіть за наявності плану, потрібні люди для його реалізації. Кадровий голод у сфері кібербезпеки залишається глобальною проблемою: у 2024 році 53% організацій повідомили про серйозний дефіцит навичок у сфері ІБ, що на 26% більше, ніж попереднього року. Цей дефіцит має вимірювані наслідки – середні збитки від порушення безпеки у компаній з нестачею ІБ-кадрів виявились на 1,76 млн дол. США більшими, ніж у компаній з укомплектованим штатом[34]. В контексті бізнесу це означає довший час ліквідації інциденту та більшу тривалість перерв у роботі. Окрім того, обмежений бюджет на кібербезпеку теж грає роль: за даними SANS, нестача фінансування залишається серед топових викликів для команд реагування. Якщо організація недоінвестовує в системи захисту та персонал, інциденти лишаються непоміченими довше, а реагування на них відбувається повільніше, що прямо загрожує безперервності бізнес-процесів.

Затримки у виявленні інцидентів (довгий MTTD). *Mean Time to Detect* – середній час виявлення загрози – у багатьох компаній вимірюється не годинами, а місяцями. Світова статистика свідчить, що в 2024 році компанії в середньому витрачали 204 дні на ідентифікацію порушення та ще 73 дні на його стримування. Тобто життєвий цикл інциденту (від проникнення зловмисника до повної ліквідації) сягає ~277 днів[35]. Така затримка означає, що бізнес може майже 9 місяців працювати під впливом атаки – з витоком даних, порушенням процесів, прихованими збоями. Природно, чим довше інцидент лишається неусунутим, тим більший збиток він спричиняє. Наприклад, якщо вдається локалізувати та усунути порушення швидше ніж за ~200 днів, середній збиток складає ~3,61 млн дол. США; якщо ж інцидент тягнеться довше 200 днів – втрати зростають до ~4,87 млн дол. США[36]. Відповідно, несвоєчасне виявлення – наслідок прогалин у моніторингу та відсутності цілодобового SOC – прямо впливає на безперервність бізнесу. Поки атака не виявлена, зловмисники можуть порушувати роботу систем, викрадати дані, а компанія цього не розуміє і не реагує.

Недостатня координація та комунікації під час інциденту. Ще одним поширеним недоліком є інформаційні силоси між підрозділами та брак налагоджених каналів зв'язку під час кризової ситуації. Якщо відділи ІТ, безпеки, підтримки бізнесу діють розрізнено, це ускладнює одночасне вирішення проблеми. Наприклад, ІТ-відділ може перезавантажувати сервери, не повідомивши службу безпеки, або відсутнє сповіщення керівництва про критичний інцидент. Досвід показує, що невизначеність і роз'єднаність у комунікаціях під час інциденту призводять до дублювання зусиль, помилок або зайвих простоїв. Важливо, щоб була створена єдина команда або принаймні централізований координаційний центр реагування, куди стекатиметься інформація і звідки розподілятимуться завдання[37]. Інакше навіть незначний інцидент може розрости до кризи через неправильно скоординовані дії, що зупиняють бізнес-операції.

Недотримання повного циклу реагування (без навчання на інцидентах). Багато організацій сфокусовані лише на гасінні "пожежі", тобто усуненні поточного інциденту, і не аналізують його після завершення. Відсутність етапу *lessons learned* (роботи над помилками) – теж серйозний недолік. Якщо після інциденту компанія не робить розслідування причин, не оновлює політики і не навчає персонал на основі отриманого досвіду, то ті самі вразливості можуть бути використані повторно. Постінцидентний аналіз дає змогу виявити, що спрацювало добре, а що ні, та вдосконалити процес реагування надалі. Натомість його ігнорування позбавляє організацію можливості підвищити свою стійкість. У підсумку компанія залишається вразливою до аналогічних атак, що знову загрожує перервами в роботі. Це замкнене коло: *недопрацьований процес -> повторний інцидент -> новий збій бізнесу*[38].

Вплив недоліків на безперервність бізнесу. Перераховані проблеми управління ІІБ мають кумулятивний негативний ефект. Коли відсутній план, не вистачає фахівців, загрози виявляються із запізненням, а дії команди розрізнені – неминуче зростає тривалість та масштаб порушення бізнес-процесів. Статистика IBM свідчить, що ~70% організацій відзначили суттєві або дуже

суттєві перебої в роботі після кіберінциденту[36]. Іншими словами, більшість компаній відчувають значний вплив на операційну діяльність через кібератаки. Особливо це стосується випадків, коли управління інцидентом було неефективним. Бізнес може зупинятися на години чи дні (наприклад, падіння онлайн-сервісів, простої виробництва), втрачати клієнтів та доходи. Репутаційні втрати також дуже відчутні: дослідження показують, що 63% організацій втрачають існуючих клієнтів після масштабного інциденту, і відновлення довіри є надзвичайно складним[39]. Отже, недоліки в реагуванні на ІІБ фактично підривають стійкість бізнесу. Якщо компанія не в змозі швидко оговтатися від атаки, вона ризикує не лише прибутками, але й самим існуванням на ринку. Недарма довгострокова статистика свідчить: 95% компаній, що не приділяють належної уваги безперервності діяльності, банкрутують протягом першого року роботи[35]. Цей приголомшливий показник підкреслює, що у сучасному середовищі “виживають” ті організації, які завчасно готуються до інцидентів і мінімізують свої вразливості. Виявлені недоліки необхідно усувати шляхом впровадження кращих практик та рекомендацій з кібербезпеки, про що йдеться у підрозділі 3.2.

3.2 Рекомендації щодо забезпечення інформаційної безпеки та безперервності бізнесу підприємства

Для підвищення кіберстійкості підприємства та забезпечення безперервності бізнес-процесів необхідно усунути згадані вище недоліки шляхом впровадження сучасних підходів до управління ІІБ. Нижче сформульовано ключові рекомендації та найкращі практики (best practices), дотримання яких дозволить мінімізувати вплив кіберінцидентів на діяльність компанії. Ці рекомендації охоплюють як організаційні заходи, так і технічні рішення та процесні вдосконалення.

Розробка та впровадження формального плану реагування на інциденти. Кожне підприємство повинно мати актуальний документований план Incident

Response Plan (IRP), який визначає покрокові дії при кіберінцидентах. План має включати склад команди реагування (CSIRT), контактну інформацію, процедури ескалації, сценарії реагування для різних типів атак (вірус, DDoS, витік даних тощо) та методи відновлення систем. Регулярне тестування плану – обов'язкова умова: проведення навчальних кібервчень, *tabletop*-тренувань, імітація інцидентів для перевірки дієвості IRP. Досвід показує, що організації, які мають план та періодично його відпрацьовують, значно краще переносять атаки. Згідно зі звітом IBM, компанії з підготовленою командою і протестованим планом реагування мали середню вартість інциденту 3,26 млн дол. США, що на 58% менше, ніж 5,29 млн дол. США у тих, хто не мав команди і плану[36]. Тобто інвестиції у розробку та підтримку IRP прямо окупаються за рахунок зменшення збитків. Рекомендовано також узгодити план реагування з планами безперервності бізнесу (BCP, *Business Continuity Plan*) та планами відновлення після аварій (DRP), щоб дії з кібербезпеки враховували пріоритети підтримки ключових бізнес-функцій[33].

Чіткий розподіл ролей і відповідальності; налагодження комунікації. В рамках плану необхідно визначити команду реагування (наприклад, Computer Security Incident Response Team – CSIRT)[40] та закріпити ролі: хто є керівником при інциденті, хто відповідає за технічну ліквідацію, хто комунікує з керівництвом і зовнішніми сторонами, тощо. Кожен співробітник має розуміти свою зону відповідальності. Варто заздалегідь підготувати контакти необхідних осіб (внутрішніх фахівців, постачальників IT-послуг, правоохоронних органів, CERT тощо)[41] і процедуру оповіщення. Під час кризової ситуації критично важливо уникнути хаосу – тому система оповіщення і збору команди має бути відпрацьована (наприклад, дзвінком, через месенджер або автоматизовано). Комунікація з бізнес-підрозділами теж повинна бути оперативною: якщо інцидент зачіпає роботу відділів, вони мають отримувати оновлення і рекомендації (наприклад, тимчасово використовувати резервні канали, переключитись на запасні сервери тощо). Налагоджена взаємодія гарантує, що

бізнес продовжує працювати навіть під час інциденту, хоч і в обмеженому режимі, а після усунення загрози швидко повертається до норми.

Посилення моніторингу та швидкого виявлення загроз. Щоб суттєво зменшити час “невидимого” перебування зловмисника в мережі, рекомендується впровадити сучасні засоби кібермоніторингу. Ідеальним є створення або аутсорсинг центру моніторингу безпеки (SOC), який працює 24/7 і відстежує аномалії. Слід використовувати системи виявлення вторгнень (IDS/IPS), SIEM-платформи для кореляції подій, засоби моніторингу цілісності файлів, тощо. Важливим трендом є впровадження технологій XDR (Extended Detection and Response), що об’єднують телеметрію з різних джерел (мережа, кінцеві точки, хмара) для швидкого виявлення комплексних атак. За даними опитувань, дедалі більше компаній застосовують XDR-рішення і інтегрують загрозову аналітику (threat intelligence) у свої процеси[42]. У результаті зростає відсоток інцидентів, які виявляються впродовж 24 годин з моменту атаки. Швидке сповіщення про інцидент дає змогу негайно розпочати реагування і знизити збитки. Також рекомендовано налаштувати автоматизовані алерти: приміром, при виявленні несанкціонованого входу або аномального трафіку – автоматично створюється інцидент і відповідальна команда отримує повідомлення.

Використання засобів автоматизації та AI для реагування. Сучасні інструменти можуть значно прискорити реагування на інциденти та зменшити навантаження на персонал. Рекомендується впроваджувати платформи SOAR (Security Orchestration, Automation and Response), які автоматизують типові дії: збір логів, ізоляцію зараженого хоста від мережі, блокування підозрілих облікових записів тощо. Також все більшої популярності набувають рішення на основі штучного інтелекту для аналізу трафіку і поведінки. Згідно з даними IBM, застосування AI та автоматизації дозволяє зекономити в середньому 2,2 млн дол. США при інциденті за рахунок швидшого виявлення і стримування загроз. Компанії, що впровадили AI-рішення, змогли скоротити середню тривалість життєвого циклу інциденту майже на 100 днів[43]. Таким чином, інвестиції в автоматизацію реагування безпосередньо підсилюють безперервність бізнесу:

загрози гасяться більш оперативно, поки не завдали серйозної шкоди. Важливо також оцінювати окупність таких інвестицій: будувати бізнес-кейси, які демонструють, як автоматизація знизить ризики простою (що особливо актуально для керівництва, яке виділяє бюджети).

Підготовка персоналу та підвищення обізнаності. Людський фактор залишається одним із визначальних як у виникненні, так і в подоланні інцидентів. Рекомендація – регулярно навчати співробітників діям під час кіберінцидентів. Це стосується не лише команди ІБ, але й ІТ-персоналу та керівників підрозділів. Варто проводити тренінги з практичними сценаріями: наприклад, що робити, якщо помічено підозрілий лист (для Service Desk), як діяти, якщо сервер під атакою (для ІТ-адмінів), як забезпечити роботу відділу при відмові ІТ-систем (для менеджерів). Співробітники мають знати, до кого звернутися і які перші кроки зробити. Також слід підвищувати кіберобізнаність всіх працівників щодо соціальної інженерії, фішингу, щоб зменшити ймовірність інцидентів. Інвестиції в людський капітал напряму впливають на швидкість та злагодженість реагування: навчена команда здатна діяти впевнено, що скорочує показники *MTTD/MTTR*. За результатами опитування Devo/SANS, 36,4% організацій планують у найближчі 12 місяців посилювати реагування саме через додаткове навчання і сертифікацію персоналу – це визнається одним з найважливіших напрямів покращення кіберстійкості[44].

Вдосконалення процедур стримування та відновлення (Containment & Recovery). На етапі стримування інциденту важливо швидко локалізувати вплив – ізолювати уражені системи, перевести сервіси на резервні потужності. Рекомендується мати резервні копії даних та резервне обладнання, щоб у разі інциденту можна було розгорнути критичні сервіси в іншому середовищі. План безперервності бізнесу має передбачати сценарії роботи в аварійному режимі: напряму, якщо основна база даних відключена через атаку – використати резервну копію або хмарний сервіс; якщо знеструмлено дата-центр – перемкнутися на запасний майданчик. Такі заходи забезпечують життєздатність бізнес-функцій навіть під час кіберкризи. Після стримування слід оперативно

переходити до відновлення: план відновлення повинен визначати пріоритети (що відновлюємо спершу – наприклад, систему обліку чи сайт для клієнтів), цільові показники RTO/RPO для кожної системи. Чітке дотримання цих процедур дозволяє значно скоротити час простою. Наприклад, компанії, які мали наперед підготовлені *disaster recovery*-плани, змогли відновити важливі сервіси за лічені години після атак на кшталт рансомware, тоді як непідготовлені відновлювались тижнями[45].

Співпраця з зовнішніми організаціями та обмін інформацією. Рекомендується налагодити контакти з національними та галузевими структурами кіберзахисту. В Україні слід співпрацювати з CERT-UA, Держспецзв'язку, Національним координаційним центром кібербезпеки при РНБО[46]. У разі серйозного інциденту варто повідомляти компетентні органи – це не лише вимога законодавства для критичних сфер, а й практична допомога. Зовнішні експерти можуть надати інтелект про актуальні загрози, допомогти у розслідуванні. До того ж, взаємодія з правоохоронними органами (наприклад, кіберполіцією) у випадку ransomware може сприяти ідентифікації та притягненню зловмисників. За даними IBM, залучення правоохоронців до реагування на ransomware-інциденти дозволяє зменшити збитки приблизно на 470 тис. дол. США і скоротити тривалість простою на 33 дні. Також варто долучатися до інформаційних обмінів про інциденти в межах галузевих співтовариств, TRUST-груп – це підвищує проактивність захисту. Своєчасне отримання сповіщень про нові методи атак чи вразливості дає змогу попередити інцидент ще до того, як він станеться на підприємстві.

Регулярний аналіз та поліпшення процесу (цикл PDCA)[47]. Управління інцидентами – це безперервний процес, який потребує постійного вдосконалення. Рекомендується після кожного серйозного інциденту проводити ретроспективу: що спрацювало добре, що можна покращити. На основі цього слід оновлювати план реагування, навчальні матеріали, можливо – впроваджувати додаткові засоби захисту. Окрім цього, варто проводити періодичні аудити готовності: оцінювати показники ефективності реагування

(кількість інцидентів, середній час на кожну фазу IR, відсоток інцидентів, вирішених за час менший за цільовий тощо). Такі метрики допомагають виявити “вузькі місця”. За результатами опитування SANS 2023, частка компаній, що регулярно оцінюють зрілість свого процесу IR за допомогою внутрішніх або публічних метрик (наприклад, NIST CSF), зросла порівняно з 2019 роком. Це позитивна тенденція, адже неможливо покращити те, що не вимірюється. Впровадження циклу PDCA (Plan-Do-Check-Act) для процесу реагування гарантує його поступову оптимізацію.

Перераховані рекомендації можна узагальнити наступним чином: підприємство має проактивно готуватися до кіберінцидентів, вкладати ресурси у превентивні заходи (підготовку планів, резерви, навчання), а також у здатність швидко реагувати і відновлюватися. Важливо розуміти, що кібербезпека тісно пов’язана з безперервністю бізнесу. Тому заходи ІБ слід інтегрувати з загальною системою управління безперервністю діяльності. Лише цілісний, комплексний підхід – від людей до технологій – забезпечить належний рівень захисту.

Узагальнені результати та очікувані ефекти від впровадження зазначених рекомендацій наведено в таблиці 3.2 нижче. У наступному підрозділі розглянуто, яких результатів може досягти компанія, імплементувавши наведені рекомендації, та як це відобразиться на показниках безперервності її бізнес-процесів.

Таблиця 3.2

Ключові напрями вдосконалення реагування на ІІБ

№	Напрям	Ключові заходи	Очікуваний ефект / Переваги
1	Розробка формального IRP	Створення Incident Response Plan, сценарії атак, ролі, ескалація, відновлення; регулярні тренування	Зниження середньої вартості інциденту на 58%; скорочення тривалості кризи
2	Чіткий розподіл ролей і комунікація	Структура CSIRT, відповідальні особи, внутрішня та зовнішня комунікація, система оповіщення	Уникнення хаосу, швидке реагування, підтримка бізнес-процесів у кризу
3	Посилення моніторингу (SOC, XDR)	IDS/IPS, SIEM, XDR, цілодобовий моніторинг, алерти, інтеграція threat intelligence	Виявлення інцидентів упродовж 24 годин, зниження тривалості “невидимості” атак

Продовження таблиці 3.2

№	Напрям	Ключові заходи	Очікуваний ефект / Переваги
4	Автоматизація та AI-рішення	SOAR-платформи, AI-аналітика трафіку, блокування, ізоляція, автоалерти	Скорочення витрат на $2,2 млн, зменшення життєвого циклу інциденту на ~100 днів
5	Підготовка персоналу	Тренінги, сценарії, інструктажі для IT, ІБ і бізнесу, підвищення обізнаності	Зменшення MTTD/MTTR, підвищення злагодженості дій, менше помилок
6	Процедури стримування та відновлення	RTO/RPO, резерви, DRP, ізоляція, переключення на резервні потужності	Відновлення сервісів за години, мінімізація простоїв
7	Зовнішня співпраця (CERT-UA, НКЦК)	Інформування компетентних органів, взаємодія з кіберполіцією, обмін загрозами	Мінус $470 тис. збитків, скорочення простою на 33 дні
8	PDCA-цикл удосконалення IR	Ретроспективи, метрики, аудит, оновлення планів, використання NIST CSF	Постійна оптимізація процесу, зростання зрілості реагування

3.3 Ефект від імплементації рекомендацій щодо управління інцидентами інформаційної безпека та оцінка впливу на безперервність бізнесу підприємства

Впровадження описаних вище рекомендацій дозволить суттєво підвищити ефективність кіберзахисту і мінімізувати збої у роботі бізнесу. На основі звітів IBM Security X-Force Threat Intelligence Index 2024, Arctic Wolf Cybersecurity Report та досвіду компаній Nova Poshta, ПриватБанк та Київстар, можна оцінити очікуваний ефект. Нижче наведено ключові результати, яких досягають організації після імплементації кращих практик IR, та їх вплив на безперервність бізнесу.

Для скорочення часу реакції та простоїв потрібен чіткий план і тренована команда дозволяють значно зменшити *MTTD/MTTR* – середній час виявлення та ліквідації загрози. Це прямо впливає на тривалість простою бізнес-процесів. Якщо раніше, як згадувалося, інцидент міг тривати 9 місяців, то після

впровадження сучасних засобів моніторингу та автоматизації життєвий цикл інциденту скорочується на порядки. Наприклад, компанії, що запровадили XDR та AI-аналіз, зменшили загальний час реагування приблизно на 30-40%, а деякі – майже на 100 днів порівняно із середнім показником. Відповідно, бізнес-операції відновлюються швидше, а втрати від простоїв знижуються. Показовою є оцінка від Ponemon Institute: кожен зекономлений день в реагуванні економить сотні тисяч доларів потенційних збитків. Таким чином, вкладення в швидкість реагування на інциденти мають прямий фінансовий і операційний ефект – менше часу системи не працюють, менше незавершених транзакцій, вищий рівень обслуговування клієнтів[48, 49].

Задля зменшення прямих фінансових збитків від інцидентів необхідно ефективно управляти інцидентами, що значно знижить вартість кожного інциденту для підприємства. Це досягається як за рахунок скорочення масштабу атаки (вчасне стримування не дає загрозі поширитися на всі системи), так і завдяки меншим витратам на відновлення. Впровадження плану IR, як вже згадувалося, дає економію до 58% витрат при інциденті. Також, якщо компанія готується заздалегідь (резервує ресурси, налаштовує бекапи), то при реальному інциденті уникає штрафів і втрат. Наприклад, готовність до ransomware (офлайн-бекапи, розроблений план дій) може вберегти від необхідності сплачувати викуп або зупиняти виробництво на довгий термін. За оцінками FEMA (Federal Emergency Management Agency), кожен долар, інвестований у превентивні заходи, дозволяє заощадити до 7 доларів США на ліквідацію наслідків інциденту[38]. Це надзвичайно високий коефіцієнт ROI, який демонструє фінансову доцільність проактивних заходів безпеки. Отже, імплементація рекомендацій напряму підсилює фінансову стійкість бізнесу перед кіберзагрозами.

Покращення показників бізнесу та конкурентоспроможності. Компанії, що успішно управляють кіберінцидентами, зберігають довіру клієнтів та репутацію, на відміну від тих, що зазнають публічних провалів. Як зазначалося, після витоків даних клієнти втрачають довіру (63% компаній втрачали клієнтів).

Вживаючи рекомендованих заходів (особливо щодо захисту даних і швидкого інформування про інциденти)[50], підприємство може мінімізувати репутаційні втрати. Більш того, воно демонструє партнерам і клієнтам свою надійність. Дослідження свідчать, що після кризи компанії з ефективним кризовим менеджментом відновлюють свою діяльність на 53% швидше за конкурентів. Це означає швидше повернення до повноцінного обслуговування клієнтів, виконання зобов'язань та виходу на планові фінансові показники. В довгостроковій перспективі такі компанії більш стійкі – вони менше втрачають частку ринку навіть після серйозних інцидентів. Натомість недостатня готовність може коштувати дуже дорого: погано керовані кризи призводять до втрати до 15% ринкової частки підприємства. Тому впровадження найкращих практик управління інцидентами не лише захищає існуючий бізнес, а й надає підприємству конкурентну перевагу перед іншими організаціями.

Виконання нормативних вимог та уникнення санкцій. Імплементація рекомендацій також допомагає відповідати вимогам законодавства та регуляторів щодо кібербезпеки і безперервності. Для багатьох галузей (фінанси, зв'язок, критична інфраструктура) нормативні акти вимагають наявності планів реагування, проведення навчань, звітування про інциденти тощо. Виконання цих вимог підвищує рівень кіберзахисту і убезпечує від можливих штрафів чи заходів впливу з боку регуляторів. Наприклад, НБУ вимагає від банків планів забезпечення безперервності і регулярних тестувань резервних сценаріїв. Компанія, яка запровадила відповідні політики, не лише захищає себе, а й демонструє відповідність аудиторам та контролюючим органам. Таким чином, рекомендації з підрозділу 3.2 сприяють і правовій стійкості бізнесу – зменшують ризики порушення норм та пов'язаних з цим збоїв (наприклад, примусової зупинки діяльності до усунення порушень безпеки)[51].

Формування культури кіберстійкості в організації. Дотримання всіх перелічених заходів поступово формує в компанії культуру проактивної безпеки і безперервності. Співробітники усвідомлюють важливість кібербезпеки, менеджмент розглядає її як невід'ємну частину бізнес-процесів. Це веде до того,

що кіберризики враховуються при прийнятті бізнес-рішень, а у разі інциденту всі залучені сторони діють злагоджено і спокійно, згідно з планом. Кіберстійка організація краще адаптується до нових загроз: наприклад, оперативно встановлює патчі при появі критичних вразливостей, підсилює захист при отриманні попереджень від розвідки про можливі атаки. У кінцевому підсумку це означає, що кількість успішних інцидентів зменшується, а ті, що трапляються, не переростають у катастрофи. Бізнес таких організацій демонструє стійкість, або ж нестабільність функціонування є короткочасною і контрольованою.

Узагальнено ефект від імплементації рекомендацій щодо управління інцидентами наведено у таблиці 3.3

Таблиця 3.3

Ефект від імплементації рекомендацій щодо управління інцидентами

Показник	Ефект від впровадження рекомендацій
Час реагування на інциденти	Скорочення на 30–40% (до 100 днів)
Фінансові витрати	Зниження до 58%, ROI ≈ 1:7
Відновлення бізнесу	Швидше на 53%, менша втрата ринкової частки (до 15%)
Репутація і довіра	Мінімізація репутаційних втрат, збереження клієнтів
Відповідність регуляторам	Уникнення штрафів та санкцій, забезпечення правової стійкості
Культура кіберстійкості	Формування проактивного підходу до безпеки, менше інцидентів

Отже, ефект від імплементації рекомендацій проявляється у вигляді підвищеної готовності до будь-яких кібернебезпек. Компанія набуває резильєнтності – здатності швидко відновлюватися після збоїв. Якщо раніше ІІБ міг поставити бізнес на коліна, то після впровадження належного управління він стає керованою ситуацією, яку команда здатна вирішити з мінімальними втратами. Умовно кажучи, організація переходить з розряду *жертви обставин* у розряд *проактивного гравця*, який може протистояти навіть серйозним

кіберкризам. Безперервність бізнесу при цьому значно зміцнюється: критичні процеси не зупиняються або швидко відновлюються, фінансова та репутаційна шкода значно менша.

Варто наголосити, що наведені покращення не є одноразовою акцією – це постійний процес розвитку системи кібербезпеки. Загрози еволюціонують, тож і підхід до інцидент-менеджменту має вдосконалюватися. Проте фундамент закладається саме впровадженням вищезгаданих принципів. Як свідчить практика, організації, які серйозно інвестують у кібербезпеку та безперервність, виграють у довгостроковій перспективі: вони рідше зазнають масштабних збоїв, легше переносять кризи і швидше повертаються до розвитку після інцидентів, тоді як менш підготовлені конкуренти витрачають сили на ліквідацію наслідків. У підсумку, якісне управління ІІБ стає запорукою стабільності та сталого функціонування бізнесу.

Висновки до розділу 3

У розділі 3 було проаналізовано типові проблеми управління ІІБ на підприємствах та запропоновано комплекс рекомендацій для підвищення ефективності реагування з метою забезпечення безперервності бізнесу. Основні висновки можна сформулювати наступним чином:

Недоліки в управлінні ІІБ суттєво підривають безперервність бізнесу. Відсутність планів реагування, брак підготовки персоналу, повільне виявлення атак та інші прорахунки призводять до затримок у ліквідації загроз. Як наслідок, компанії переживають тривалі простої, втрачають дані, гроші та клієнтів. Статистично доведено зв’язок між слабкою підготовкою до інцидентів і масштабом збитків від них. Кіберінциденти, яким не змогли вчасно зарадити, можуть поставити під загрозу подальше існування бізнесу.

Запропоновані рекомендації дозволяють мінімізувати вплив інцидентів на діяльність підприємства. Йдеться про впровадження проактивних заходів: створення планів IRP та BCP, формування навченого CSIRT, налагодження моніторингу 24/7, використання автоматизованих інструментів реагування,

резервування ресурсів та ін. Важливою є інтеграція кібербезпеки зі стратегією безперервності – щоб IT-безпека та бізнес підрозділи діяли злагоджено під час кризових ситуацій. Рекомендації базуються на міжнародних стандартах (NIST, ISO 27035), галузевих дослідженнях та кращому досвіді провідних компаній.

Імплементація цих заходів значно підвищує рівень кіберстійкості і резильєнтності бізнесу. Підприємства, які дотримуються зазначених практик, демонструють суттєве скорочення середнього часу реагування на інциденти, зменшення фінансових втрат і відсутність критичних простоїв. Крім того, вони краще задовольняють вимоги регуляторів та зберігають довіру клієнтів, що позитивно позначається на їхній ринковій позиції навіть в умовах зростання кіберзагроз.

Загалом якісне управління ІІБ – це наріжний камінь безперервності бізнесу в цифрову епоху. Організації, які інвестують у підготовку до інцидентів, отримують не лише кібернетичну безпеку, але й бізнес-вигоди у вигляді стабільної роботи, фінансової економії та конкурентної переваги. Таким чином, реалізація представлених рекомендацій є необхідною умовою захисту підприємства від сучасних кіберризиків та забезпечення його сталого функціонування на ринку навіть за несприятливих обставин. Найкраща стратегія – бути готовим до найгіршого, аби гарантувати безперервність і успіх бізнесу за будь-яких умов.

ВИСНОВКИ

1. Досліджено актуальний стан проблеми: встановлено, що в умовах зростання кіберзагроз та дедалі більшої залежності підприємств від цифрових технологій навіть поодинокі інциденти інформаційної безпеки здатні спричинити серйозні перебої в роботі бізнес-процесів. Кількість кібератак постійно зростає, а їхні наслідки призводять до значних фінансових втрат і витрат на ліквідацію інцидентів та відновлення інфраструктури.

2. Проаналізовано природу ІІБ та їхній вплив на безперервність бізнесу: показано, що сучасні кібератаки (від масштабних вірусних епідемій, наприклад NotPetya, до таргетованих атак здирників) можуть миттєво призупинити діяльність компаній. Встановлено, що системна підготовка (класифікація інцидентів, наявність планів реагування) і оперативне реагування із застосуванням методів стримування (ізоляція уражених систем, резервне відновлення) значно зменшують негативний вплив атак.

3. Досліджено методи стримування та управління ІІБ: визначено, що ключовим етапом є своєчасна локалізація загрози (ізоляція уражених систем, блокування атакувального трафіку тощо), що дозволяє мінімізувати збитки. Аналіз практичних кейсів підтвердив ефективність цих підходів: своєчасне стримування DDoS-атак і вірусу Petya дозволяло уникнути тривалих простоїв, тоді як запізніле реагування призвело до масштабніших руйнувань інфраструктури (як у випадку атаки на «Київстар»). Підкреслено необхідність напрацьованих сценаріїв стримування для різних типів інцидентів та наявності ресурсів (резервні канали, навчений персонал, контакти з CERT тощо) для їх реалізації.

4. Вивчено показники ефективності реагування на інциденти (середній час виявлення – MTTD, середній час відновлення – MTTRestore, витрати на відновлення) та методи їх оцінювання. Встановлено, що контроль і скорочення цих метрик (зокрема MTTD і MTTR) сприяє зменшенню масштабу збитків:

підприємства зі зрілою системою реагування демонструють значно нижчі середні часи реагування і відповідно менші фінансові втрати.

5. Сформульовано практичні рекомендації щодо оптимізації показників реагування: обґрунтовано необхідність розробки формальних планів реагування (IRP/BCP), проведення регулярних навчань і тренінгів персоналу, створення цілодобових центрів моніторингу з навченими командами реагування (CSIRT), а також впровадження автоматизації процесів виявлення загроз, резервування критичних ресурсів та інтеграції кібербезпеки зі стратегією безперервності бізнесу. Зазначено, що дотримання цих заходів, які базуються на кращих галузевих практиках і стандартах (NIST, ISO 27035), дозволяє підприємствам скоротити час простою, мінімізувати втрати та зберегти довіру клієнтів навіть під час складних кібератак.

6. Встановлено узагальнюючі висновки і рекомендації: встановлено, що високий рівень організаційної зрілості і зріла система реагування на інциденти є запорукою стійкого функціонування бізнесу: впровадження розроблених підходів (планування інцидент-менеджменту, тренування персоналу, моніторинг, резервування) призводить до суттєвого скорочення середніх часів реагування та фінансових втрат. Обґрунтовано, що інформаційну безпеку слід розглядати як невід’ємну частину управління операційною стійкістю: інтеграція процесів реагування на інциденти з планами забезпечення безперервності (BCP/DRP) дає підприємствам змогу витримувати кіберудари і продовжувати роботу без критичних перебоїв.

Таким чином, виконане дослідження підтверджує необхідність проактивного і системного підходу до управління ІБ-інцидентами. Запропоновані в роботі рішення і рекомендації можуть бути використані для підвищення кіберстійкості підприємств: їх імплементація дозволяє значно зменшити наслідки атак, забезпечивши надійну безперервність бізнес-процесів в умовах зростання цифрових загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ukraine’s Ukrzaliznytsia railway operator hit by cyberattack, ticket system disrupted. Industrial Cyber [Електронний ресурс]. – Режим доступу: https://industrialcyber.co/transport/ukraines-ukrzaliznytsia-railway-operator-hit-by-cyberattack-ticket-system-disrupted-sparking-long-queues/

2.Data breaches 2024: Reports and statistics. HelpNetSecurity [Електронний ресурс]. – Режим доступу: https://www.helpnetsecurity.com/2025/01/02/data-breaches-2024-reports/

3.Ransomware fallout: 94% of attacks now involve data exfiltration. HelpNetSecurity [Електронний ресурс]. – Режим доступу: https://www.helpnetsecurity.com/2024/05/23/ransomware-attacks-data-exfiltration/

4.Security incident recovery times are over 7 months on average. ITPro [Електронний ресурс]. – Режим доступу: https://www.itpro.com/security/security-incident-recovery-times-are-over-7-months-on-average

5.A June cyberattack that snarled shipping giant Maersk cost it $300 million. Los Angeles Times [Електронний ресурс]. – Режим доступу: https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html

6.Іванішин С. В. Стримування ІІБ в контексті безперервності бізнесу / С. В. Іванішин // Кібербезпека: освіта, наука, техніка. – 2023. – № 4. – С. 72–80. – [Електронний ресурс]. – Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/download/692/559/2297

7.Business interruption: the fastest-growing cyberattack cost. Iwins [Електронний ресурс]. – Режим доступу: https://www.iwins.com/business-interruption-the-fastest-growing-cyberattack-cost/

8.Containment in incident response: The art of stopping the bleed. LinkedIn / Mathew Davis [Електронний ресурс]. – Режим доступу: https://www.linkedin.com/pulse/containment-incident-response-art-stopping-bleed-mathew-davis-tpmie

9.Incident response containment. ReliaQuest [Електронний ресурс]. – Режим доступу: https://reliaquest.com/cyber-knowledge/incident-response-containment/

10.Containment strategies. Saylor Academy [Електронний ресурс]. – Режим доступу: https://learn.saylor.org/mod/book/tool/print/index.php?id=29706&chapterid=5350

11.Survey IR 2023. Devo [Електронний ресурс]. – Режим доступу: https://www.devo.com/wp-content/uploads/2023/10/Survey_IR-2023_Devo.pdf

12.Cost of a Data Breach Report 2023. The Hacker News [Електронний ресурс]. – Режим доступу: https://thehackernews.com/2023/12/cost-of-data-breach-report-2023.html

13.Top 10 cybersecurity metrics and KPIs. Mimecast [Електронний ресурс]. – Режим доступу: https://www.mimecast.com/blog/top-10-cybersecurity-metrics-and-kpis/

14.The real cost of a data breach. Field Effect [Електронний ресурс]. – Режим доступу: https://fieldeffect.com/blog/real-cost-data-breach

15.How to measure incident response effectiveness. Supaste [Електронний ресурс]. – Режим доступу: https://www.supaste.co.uk/how-to-measure-incident-response-effectiveness/

16.Lancope-Ponemon Report: Cyber Security Incident Response. Ponemon Institute [Електронний ресурс]. – Режим доступу: https://www.ponemon.org/local/upload/file/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf

17. АТ КБ «ПриватБанк». Інтегрований річний звіт, 2023 [Електронний ресурс]. – Режим доступу: https://dwfvpbrjajjfs.cloudfront.net/media/static_files/2023_Integrated_Report_PrivatBank.pdf

18.Нова пошта назвала вірус, який атакував компанію [Електронний ресурс]. – Режим доступу: https://biz.nv.ua/ukr/markets/nova-poshta-nazvala-atakuvav-kompaniju-virus-1391915.html

19.Як Київстар відновлювався після наймасштабнішої атаки в історії України [Електронний ресурс]. – Режим доступу: https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/

20.Рада національної безпеки і оборони України. Аналітичний звіт про кібербезпеку: січень–березень 2024 [Електронний ресурс]. – Режим доступу: https://www.rnbo.gov.ua/files/НКЦК/2024/20240422_Cyber%20%E2%80%8B%E2%80%8Bsecurity%20January-March%202024/UFSS_QASummary_Q2_2024.pdf

21.Кібератака на ПриватБанк, Ощадбанк та сайт Міноборони [Електронний ресурс]. – Режим доступу: https://kg.ua/news/kiberataka-na-privatbank-oshchadbank-ta-sayt-minoboroni-robotu-bankivskih-veb-resursiv

22.Новая пошта відновила роботу після вірусу Petya [Електронний ресурс]. – Режим доступу: https://lb.ua/economics/2017/06/27/370202_novaya_pochta_vozobnovila_rabotu.html

23.Хакери перебували в системі Київстар з травня 2023 року – СБУ [Електронний ресурс]. – Режим доступу: https://forbes.ua/news/khakeri-perebuvali-v-sistemi-kiivstar-z-travnya-2023-roku-sbu-04012024-18307

24.Кібератака на «Київстар» (2023) [Електронний ресурс] // Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki/Кібератака_на_«Київстар»_(2023)

25.ПриватБанк забезпечив стабільну роботу під час кібератаки [Електронний ресурс]. – Режим доступу: https://interfax.com.ua/news/economic/1035627.html

26.Zscaler. 7 key takeaways from IBM’s Cost of a Data Breach Report 2024 [Електронний ресурс]. – Режим доступу: https://www.zscaler.com/blogs/product-insights/7-key-takeaways-ibm-s-cost-data-breach-report-2024

27.Держспецзв’язку: зафіксовано 41 мільйон кібератак [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/news/321f4bf8

28.Росіяни заявили, що це вони «поклали» Нову Пошту [Електронний ресурс]. – Режим доступу: https://www.unian.ua/russianworld/rosiyani-zayavili-shcho-ce-voni-poklali-novu-poshtu-poyasnennya-vbilo-12262254.html

29.WeSecureApp. Top 7 cybersecurity measures that enterprises shouldn’t neglect [Електронний ресурс]. – Режим доступу: https://wesecureapp.com/blog/top-7-cyber-security-measures-that-enterprises-shouldnt-neglect/

30.РНБО України. Кібердайджест №2, лютий 2024 [Електронний ресурс]. – Режим доступу: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest%2002_2024/Feb_2024_fin.pdf

31.CERT-UA. Інформація щодо реагування на кібератаки на об’єкти критичної інфраструктури України [Електронний ресурс]. – Режим доступу: https://novozzso7.school.org.ua/informaciya-schodo-adekvatnogo-ta-svoechasnogo-reaguvannya-na-kiberataki-na-ob%E2%80%99ekti-kritichnoi-infrastrukturi-ukraini-11-06-07-12-05-2022/

32. CERT-UA. Перелік категорій кіберінцидентів [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/recommendation/16904

33.Cichonski P. et al. Computer Security Incident Handling Guide. NIST SP 800-61r2 [Електронний ресурс]. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

34. SANS Institute. 2023 Survey | Incident Response [Електронний ресурс]. – Режим доступу: https://www.sans.org/white-papers/2023-survey-event-incident-response/

35.ITPro. Security incident recovery times are over 7 months on average [Електронний ресурс]. – Режим доступу: https://www.itpro.com/security/security-incident-recovery-times-are-over-7-months-on-average

36.IBM. Cost of a Data Breach Report 2024 [Електронний ресурс]. – Режим доступу: https://www.ibm.com/reports/data-breach

37. ReliaQuest. Annual Cyber-Threat Report: 2024 [Електронний ресурс]. – Режим доступу: https://reliaquest.com/resources/research-reports/annual-threat-report-2024/

38. Ponemon Institute. Cyber Security Incident Response: Are We as Prepared as We Think? [Електронний ресурс]. – Режим доступу: https://www.ponemon.org/local/upload/file/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf

39.Chokshi N. Maersk says NotPetya attack cost up to $300 million [Електронний ресурс] // Los Angeles Times. – 2017. – Режим доступу: https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html

40.ISO/IEC 27035-1:2023. Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management.

41.FEMA. Business Continuity Planning Suite [Електронний ресурс]. – Режим доступу: https://www.ready.gov/business-continuity-plan

42. Arctic Wolf. The State of Cybersecurity: 2024 Trends Report [Електронний ресурс]. – Режим доступу: https://arcticwolf.com/resource/aw/the-state-of-cybersecurity-2024-trends-report

43. Gartner. Cybersecurity Trends: Resilience Through Transformation [Електронний ресурс]. – Режим доступу: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

44.SANS Institute. 2023 Survey | Incident Response [Електронний ресурс]. – Режим доступу: https://www.sans.org/white-papers/2023-survey-event-incident-response/

45.Help Net Security. Ransomware attacks & data exfiltration 2024 [Електронний ресурс]. – Режим доступу: https://www.helpnetsecurity.com/2024/05/23/ransomware-attacks-data-exfiltration/

46. Міністерство економіки України. Кібербезпека як фактор забезпечення економічної безпеки [Електронний ресурс]. – Режим доступу: https://me.gov.ua/download/b05eaae6-bbdc-4c75-a16c-8394c37de07c/file.pdf

47. ENISA. Incident management [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/topics/incident-management

48. Help Net Security. Data breaches 2024: reports and insights [Електронний ресурс]. – Режим доступу: https://www.helpnetsecurity.com/2025/01/02/data-breaches-2024-reports/

49. Fastly. Cybersecurity at the Crossroads: Global Security Research Report 2024 [Електронний ресурс]. – Режим доступу: https://learn.fastly.com/rs/025-XKO-469/images/Fastly_Cybersecurity_at_the_Crossroads.pdf

50.Deloitte. Cyber Defense & Resilience [Електронний ресурс]. – Режим доступу: https://www.deloitte.com/global/en/services/consulting/services/cyber-defense-resilience.html

51. Національний банк України. Постанова Правління від 19 травня 2020 року № 65 «Про затвердження Положення про здійснення банками фінансового моніторингу» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/v0065500-20