МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “АНАЛІЗ ПРОЦЕСІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ”

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

_____ Єгор ДОНЦОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

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

Єгор ДОНЦОВ
Ім’я, ПРІЗВИЩЕ

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

Рецензент: Галина ГАЙДУР
Д.т.н., професор Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
"____"_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Донцову Єгору Андрійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи "Аналіз процесів управління інцидентами інформаційної безпеки організації",
керівник кваліфікаційної роботи ЯКИМЕНКО Юрій, к.в.н., доцент,
(ІПРІЗВИЩЕ, Ім'я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від 27.02.24 № 36.

2. Строк подання кваліфікаційної роботи "20" травня 2024р.

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

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати теоретичні аспекти процесів управління інцидентами інформаційної безпеки організації
4.2. Дослідити сучасні методи управління інцидентами інформаційної безпеки.
4.3. Визначити ефективність управління інцидентами інформаційної безпеки організації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

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

КАЛЕНДАРНИЙ ПЛАН

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

Здобувач вищої освіти _____ Єгор ДОНЦОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

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

Направляється здобувач Донцов Є.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Аналіз процесів управління інцидентами інформаційної безпеки організації"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ДОНЦОВ Єгор у кваліфікаційній роботі проаналізував теоретичні аспекти процесів управління інцидентами інформаційної безпеки організації, дослідив сучасні методи управління інцидентами інформаційної безпеки, визначив ефективність управління інцидентами інформаційної безпеки організації, розробив практичні рекомендації за темою дослідження.

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

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

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

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Донцов Є.А. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ДОНЦОВА Єгора
на тему " Аналіз процесів управління інцидентами інформаційної безпеки організації "

Актуальність.

Процес управління інцидентами інформаційної безпеки (УІБ) покликано забезпечити організацію можливістю своєчасного виявлення інциденту та якомога швидшого реагування на нього за допомогою обраних організаційних і технічних засобів підтримки. Аналізу інцидентів, що відбулися, завжди наділяється постійна увага з метою планування превентивних заходів захисту і поліпшення процесу забезпечення інформаційної безпеки в цілому.

Тому в умовах зростання інформаційних ризиків і загроз управління інцидентами інформаційної безпеки організації та аналіз його процесів є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено сучасні методи управління інцидентами і досвід їх використання у вирішенні проблем інформаційної безпеки

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

3. Автор опрацював значну джерельну базу: близько 50 публікацій, в тому числі англомовних.

4. За результатами дослідження запропоновано рекомендації щодо покращення управління інцидентами інформаційної безпеки організації і показано на прикладі обраної компанії.

Недоліки.

Доцільно було б приділити більше уваги програмним інструментам для оцінки ефективності управлінських процесів з питань інформаційної безпеки.

Однак, це зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент: професор кафедри
Інформаційної та кібернетичної
безпеки,
д.т.н, професор_____ Галина ГАЙДУР
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню процесів управління інцидентами інформаційної безпеки організації. Робота складається зі вступу, трьох розділів, що містять 9 рисунків, висновків і списку використаних джерел із 43 найменувань. Загальний обсяг роботи становить 70 аркушів з яких 6 аркуші займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження засад аналізу процесів управління інцидентами інформаційної безпеки організації та розробка рекомендацій щодо підвищення їх ефективності.

Об'єктом дослідження є процеси управління інформаційною безпекою організації

Предмет дослідження **-** особливості управління інцидентами інформаційної безпеки організації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, системного підходу до управління інцидентами інформаційною безпекою.

Як результат у роботі проаналізовано теоретичні аспекти процесів управління інцидентами інформаційної безпеки організації, досліджено сучасні методи управління інцидентами інформаційної безпеки, визначено ефективність управління інцидентами інформаційної безпеки організації, розроблено практичні рекомендації.

Галузь застосування. Розроблені рекомендації можуть бути використані при вдосконалення процесів управління інцидентами інформаційної безпеки організації.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ ІНЦИДЕНТАМИ, МЕТОДИ УПРАВЛІННЯ ІНЦИДЕНТАМИ, ЕФЕКТИВНІСТЬ УПРАВЛІННЯ ІНЦИДЕНТАМИ, АНАЛІЗ ІНЦИДЕНТІВ.

ABSTRACT

The qualification work is devoted to researching the processes of managing information security incidents of the organization. The work consists of an introduction, three chapters containing 9 figures, conclusions and a list of references containing 43 items. The total volume of work is 70 pages, of which 6 pages are occupied by a list of abbreviations and a list of references.

The purpose of the study is to investigate the principles of analyzing the organization's information security incident management processes and develop recommendations for improving their effectiveness.

The object of the study is the organization's information security management processes.

The subject of the study is the specifics of incident management of the organization's information security.

Research methods. To solve the above-mentioned scientific task, the methods of analysis and synthesis, comparison, classification, system approach to information security incident management are used in the work.

As a result, theoretical aspects of the organization's information security incident management processes were analyzed, modern information security incident management methods were investigated, the effectiveness of the organization's information security incident management was determined, and practical recommendations were developed.

Field of application. The developed recommendations can be used to improve the organization's information security incident management processes.

Keywords: INFORMATION SECURITY, INCIDENT MANAGEMENT, INCIDENT MANAGEMENT METHODS, INCIDENT MANAGEMENT EFFICIENCY, INCIDENT ANALYSIS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 9

ВСТУП 10

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПРОЦЕСІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ 12

1.1 Визначення інформаційної безпеки та її управління інцидентами. 12

1.2 Вимоги нормативних документів для управління інцидентами інформаційної безпеки 15

Висновки до розділу 1 26

РОЗДІЛ 2. АНАЛІЗ СУЧАСНИХ МЕТОДІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 28

2.1. Огляд сучасних методів управління інцидентами інформаційної безпеки…. 28

2.2. Аналіз досвіду використання методів управління інцидентами 35

2.3. Проблеми і виклики сучасних методів управління інцидентами 40

2.4. Методичні підходи щодо оцінки ефективності управління інцидентами інформаційної безпеки 43

Висновки до розділу 2 50

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ 52

3.1. Аналіз поточного стану управління інцидентами інформаційної безпеки організації за допомогою SWOT-аналізу (на прикладі) 52

3.2. Рекомендації щодо покращення управління інцидентами управління інформаційної безпеки організації 58

Висновки до розділу 3 62

ВИСНОВКИ 63

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 66

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ІБП	Інцидент інформаційної безпеки
ІР	Інформаційні ресурси
ІСІБ	Інформаційна система інформаційної безпеки
ІТ	Інформаційні технології
CERT	Computer Emergency Response Team (Група реагування на комп'ютерні інциденти)
CSIRT	Computer Security Incident Response Team (Група реагування на інциденти комп'ютерної безпеки)
IEC	IEC - International Electrotechnical Commission (Міжнародна електротехнічна комісія)
ISO	ISO - International Organization for Standardization (Міжнародна організація зі стандартизації)
NIST	National Institute of Standards and Technology (Національний інститут стандартів і технологій)
PDCA	Plan-Do-Check-Act (Цикл Планування-Виконання-Перевірка-Дія)
SANS	SysAdmin, Audit, Network, Security (Інститут навчання безпеки)
SIEM	Security Information and Event Management (Управління інформацією та подіями безпеки)

ВСТУП

Актуальність теми. В умовах стрімкого розвитку інформаційних технологій та зростаючої залежності організацій від інформаційних систем, забезпечення належного рівня інформаційної безпеки стає одним з ключових факторів успішного функціонування будь-якої організації. Інциденти інформаційної безпеки, такі як витоки конфіденційних даних, кібератаки, збої в роботі систем та порушення політик безпеки, можуть завдати значних збитків і негативно вплинути на репутацію організації.

Ефективне управління інцидентами інформаційної безпеки є критично важливим процесом, який дозволяє своєчасно виявляти, аналізувати, реагувати та відновлюватися від інцидентів, мінімізуючи їх негативний вплив. Належне управління інцидентами допомагає організаціям захистити свої інформаційні активи, забезпечити безперервність бізнес-процесів та дотримуватися вимог нормативних документів і стандартів у сфері інформаційної безпеки.

Проте, впровадження ефективних процесів управління інцидентами інформаційної безпеки в організаціях часто стикається з низкою проблем та викликів, таких як обмеженість ресурсів, недостатня кваліфікація персоналу, складність координації дій та відсутність чітких методик оцінки ефективності цих процесів.

Мета роботи полягає у дослідженні засад аналізу процесів управління інцидентами інформаційної безпеки організації та розробка рекомендацій щодо підвищення їх ефективності.

Об'єкт дослідження - процеси управління інформаційною безпекою організації.

Предмет дослідження - особливості управління інцидентами інформаційної безпеки організації.

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

1. Вивчити теоретичні основи інформаційної безпеки та управління інцидентами.

2. Дослідити сучасні методи управління інцидентами інформаційної безпеки.

3. Визначити ефективність управління інцидентами інформаційної безпеки організації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, системного підходу до управління інцидентами інформаційною безпекою.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу організаціям вдосконалити процеси управління інцидентами, підвищити обізнаність персоналу, покращити координацію дій та своєчасного реагування на інциденти інформаційної безпеки.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу”, яка проходила в ДУІКТ 28 лютого 2024 року.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПРОЦЕСІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Для розкриття теми кваліфікаційної роботи рекомендується розглянути теоретичні основи інформаційної безпеки та управління інцидентами. Визначити поняття інформаційної безпеки, її цілі та компоненти. Розкрити сутність управління інцидентами інформаційної безпеки, його етапи та процеси. А також проаналізувати вимоги нормативних документів, таких як стандарти ISO/IEC 27001, NIST SP 800-61 та інші, щодо впровадження процесів управління інцидентами

1.1 Визначення інформаційної безпеки та її управління інцидентами.

Інформаційна безпека є критично важливою для будь-якої організації, яка залежить від інформаційних систем та технологій. Вона охоплює захист інформації та інформаційних систем від різноманітних загроз, таких як несанкціонований доступ, витік чи модифікація даних, кібератаки та інші порушення безпеки. Забезпечення інформаційної безпеки є необхідним для підтримки конфіденційності, цілісності та доступності інформації, а також для забезпечення безперервності бізнес-процесів та дотримання нормативних вимог.

Визначення інформаційної безпеки згідно з міжнародним стандартом ISO/IEC 27001 був спільно розроблений організацією ISO (International Organization for Standardization) та IEC (International Electrotechnical Commission). Його структура охоплює комерційні, некомерційні та урядові організації. Стандарт вміщає та визначає вимоги до створення, впровадження, моніторингу та вдосконалення такого інструмента, як система менеджменту інформаційної безпеки. В його основі закладено три основні принципи.

1. Конфіденційність. Інформація, яка зберігається на підприємстві, доступна лише певному колу людей.

2. Цілісність даних. Матеріали, необхідні для успішного ведення бізнесу, надійно зберігаються та не ушкоджуються.

3. Доступність інформації. Представники та робітники організації мають доступ до даних для вільного використання у робочих цілях.

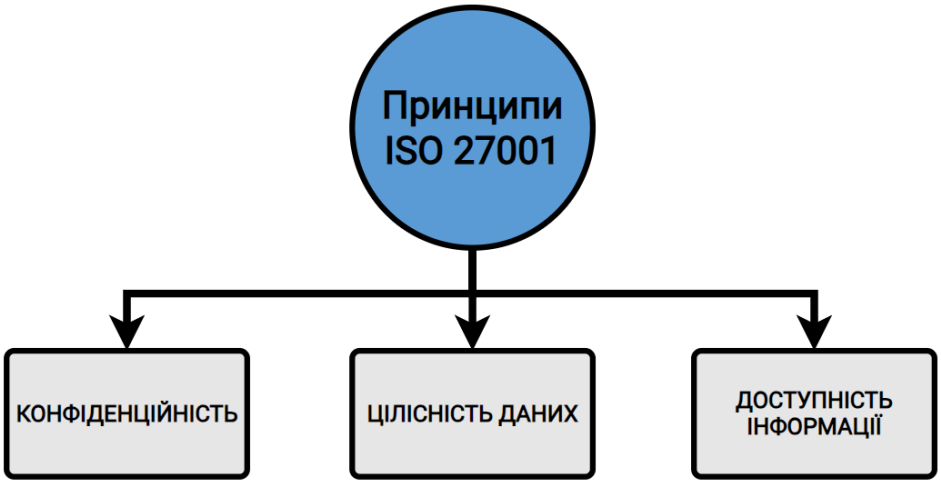


Рис. 1.1. Основні принципи стандарту ISO/IEC 27001

Управління інцидентами інформаційної безпеки є одним з ключових процесів у забезпеченні належного рівня інформаційної безпеки організації. Інцидент інформаційної безпеки визначається як будь-яка небажана або несподівана подія, що може призвести до порушення конфіденційності, цілісності або доступності інформації або інформаційних систем. Прикладами інцидентів є кібератаки, витоки даних, порушення політик безпеки, збої в роботі систем та інші події, що можуть завдати шкоди організації.

Управління інцидентами інформаційної безпеки є безперервним процесом, який зазвичай складається з чотирьох основних етапів[1]:

1. Підготовка та запобігання: На цьому етапі організація створює відповідні політики, процедури та плани реагування на інциденти, а також забезпечує підготовку персоналу та впровадження необхідних технічних засобів для виявлення та реагування на інциденти.

2. Виявлення та аналіз: На цьому етапі здійснюється моніторинг інформаційних систем та інфраструктури з метою своєчасного виявлення потенційних інцидентів. Після виявлення інциденту проводиться його аналіз для визначення характеру, масштабів та потенційного впливу.

3. Реагування та відновлення: На цьому етапі вживаються заходи для обмеження та мінімізації наслідків інциденту, а також для відновлення нормального функціонування систем і бізнес-процесів. Це може включати ізоляцію уражених систем, усунення вразливостей, відновлення даних із резервних копій тощо.

4. Аналіз після інциденту: На цьому етапі проводиться всебічний аналіз інциденту, його причин та наслідків. На основі цього аналізу розробляються рекомендації для вдосконалення процесів управління інцидентами та підвищення загального рівня інформаційної безпеки організації.

Ефективне управління інцидентами інформаційної безпеки вимагає системного підходу та залучення відповідних ресурсів, таких як кваліфікований персонал, технології для виявлення та реагування на інциденти (SIEM-системи, системи запобігання вторгненням тощо), а також чіткі процедури та плани дій.

Окрім технічних аспектів, управління інцидентами також включає організаційні та процесні складові, такі як визначення ролей і обов'язків, налагодження комунікацій та звітності, координація дій різних підрозділів організації, а також забезпечення відповідності нормативним вимогам та стандартам.

Стандарти та нормативні документи, такі як NIST SP 800-61 "Computer Security Incident Handling Guide", ISO/IEC 27035 "Information technology - Security techniques - Information security incident management" та інші, надають рекомендації та найкращі практики для впровадження ефективних процесів управління інцидентами інформаційної безпеки.[1]

Важливо зазначити, що управління інцидентами є невід'ємною частиною загальної системи управління інформаційною безпекою організації. Воно тісно пов'язане з такими процесами, як оцінка ризиків, управління безперервністю

бізнесу, управління змінами, моніторинг та аудит безпеки, а також забезпечення відповідності нормативним вимогам.[2]

Підсумовуючи, управління інцидентами інформаційної безпеки є критично важливим процесом для забезпечення належного рівня інформаційної безпеки організації. Ефективне управління інцидентами дозволяє своєчасно виявляти та реагувати на потенційні загрози, мінімізувати негативний вплив інцидентів, забезпечити безперервність бізнес-процесів та дотримуватися нормативних вимог. Це вимагає системного підходу, відповідних ресурсів та постійного вдосконалення процесів на основі аналізу інцидентів та кращих практик.

1.2 Вимоги нормативних документів для управління інцидентами інформаційної безпеки

Управління інцидентами інформаційної безпеки є важливим процесом, який регулюється низкою нормативних документів та стандартів. Дотримання цих вимог дозволяє організаціям забезпечити ефективне управління інцидентами, мінімізувати ризики та наслідки інцидентів, а також гарантувати відповідність нормативним вимогам та найкращим практикам.

Одним з ключових стандартів у сфері управління інформаційною безпекою є ISO/IEC 27001 "Інформаційні технології. Системи управління інформаційною безпекою"[3]. Цей стандарт встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ) в організації. Стандарт містить розділ, який стосується управління інцидентами інформаційної безпеки.

Відповідно до ISO/IEC 27001, організація повинна встановити відповідальність та процедури для виявлення, реагування, аналізу та вирішення інцидентів інформаційної безпеки. Крім того, організація повинна збирати та аналізувати дані про інциденти інформаційної безпеки для визначення тенденцій і вжиття відповідних дій з метою запобігання їх повторенню.

Більш детальні вимоги до управління інцидентами інформаційної безпеки викладені в стандарті ISO/IEC 27035 "Інформаційні технології. Управління інцидентами інформаційної безпеки". Цей стандарт надає рекомендації та практичні поради щодо планування, проектування, впровадження та експлуатації процесів управління інцидентами інформаційної безпеки в організаціях.

Згідно з ISO/IEC 27035, процес управління інцидентами інформаційної безпеки повинен охоплювати наступні основні етапи:

1. Підготовка до управління інцидентами
2. Виявлення та повідомлення про інциденти
3. Оцінка та вирішення інцидентів
4. Реагування на інциденти
5. Аналіз після інциденту

Стандарт детально описує вимоги та рекомендації для кожного з цих етапів, включаючи створення відповідних політик, процедур, планів реагування на інциденти, а також організаційні аспекти, такі як визначення ролей та обов'язків, навчання персоналу та забезпечення необхідними ресурсами.

Іншим важливим документом є NIST SP 800-61 "Computer Security Incident Handling Guide" (Керівництво з управління інцидентами комп'ютерної безпеки), розроблене Національним інститутом стандартів і технологій США, схематична робота зображена на рис. 1.2. Це керівництво надає детальні рекомендації щодо створення та підтримки ефективного процесу управління інцидентами інформаційної безпеки в організаціях.

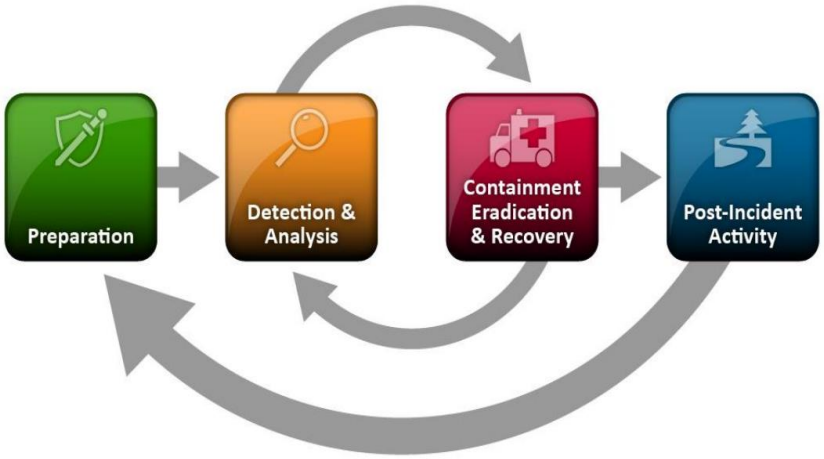


Рис 1.2. Схематична робота NIST SP 800-61 [4]

NIST SP 800-61 визначає чотири основні етапи процесу управління інцидентами:

1. Підготовка (Preparation)
2. Виявлення та аналіз (Detection & Analysis)
3. Реагування (Containment, Eradication & Recovery)
4. Постінцидентна діяльність (Post-incident Activity)

На етапі підготовці виконуються створення політик та процедур, наявність відповідного обладнання та програмного забезпечення, проведення навчання персоналу, а також визначення та надання ресурсів, необхідних для ефективного реагування на інциденти.

На другому етапі відбувається виявлення інциденту та його початковий аналіз для визначення природи і масштабів проблеми. Це включає моніторинг систем та мереж, виявлення аномалій і потенційних загроз, а також збір та аналіз відповідних даних.

Третій етап, реагування, включає в собі три підетапи, а саме:

- Стримування (Containment) – це обмеження впливу інциденту на інші системи та запобігання подальшого поширення загрози.

- Ліквідація (Eradication) – це видалення шкідливих компонентів та усунення вразливостей, які були використані при атаці.

- Відновлення (Recovery) – це відновлення систем у нормальний режим, перевірка їх на наявність загроз, що залишилися.

На останньому етапі проводиться аналіз причин інциденту та його наслідків для запобігання його в майбутньому та робиться документування інциденту.

Крім вищезазначених стандартів, існують також інші нормативні документи та настанови, які стосуються управління інцидентами інформаційної безпеки. Наприклад, SANS Institute's Incident Handler's Handbook (Посібник з управління інцидентами безпеки) надає практичні рекомендації та кейси для фахівців з управління інцидентами.

В табл. 1.1. наведено порівняння основних вимог до управління інцидентами інформаційної безпеки згідно з різними стандартами та керівництвами.

Таблиця 1.1.

Порівняння вимог до управління інцидентами інформаційної безпеки

Вимога	**ISO/IEC 27035**	**NIST SP 800-61**	**SANS Incident Handler's Handbook**
Етапи управління інцидентами	1. Підготовка 2. Виявлення та повідомлення 3. Оцінка та вирішення 4. Реагування 5. Аналіз після інциденту	1. Підготовка 2. Виявлення та аналіз 3. Реагування 4. Постінцидентна діяльність	1. Підготовка 2. Виявлення та валідація 3. Стримування та ліквідація 4. Відновлення 5. Аналіз після інциденту

Продовження таблиці 1.1.

Вимога	ISO/IEC 27035	NIST SP 800-61	SANS Incident Handler's Handbook
Створення політик та процедур	Вимагається	Вимагається	Вимагається
Створення групи реагування на інциденти	Рекомендовано	Вимагається	Вимагається
Навчання персоналу	Вимагається	Вимагається	Вимагається
Документування інцидентів	Вимагається	Вимагається	Вимагається
Звітність про інциденти	Вимагається	Вимагається	Вимагається
Аналіз після інциденту	Вимагається	Вимагається	Вимагається

Як видно з табл. 1.1., різні стандарти та керівництва мають схожі вимоги до управління інцидентами інформаційної безпеки, хоча можуть відрізнятися деталями та акцентами. Загалом, вони передбачають створення відповідних політик, процедур та планів реагування, формування групи реагування на інциденти, навчання персоналу, документування інцидентів, звітність та проведення аналізу після інцидентів для вдосконалення процесів та запобігання повторенню інцидентів.

Окрім загальних стандартів та керівництв, існують також галузеві нормативні вимоги та рекомендації щодо управління інцидентами інформаційної безпеки, які організації повинні враховувати. Наприклад, у фінансовій сфері діють вимоги Базельського комітету з банківського нагляду, в охороні здоров'я -

вимоги HIPAA (Закон про портативність та підзвітність медичного страхування), а для урядових організацій - вимоги FISMA (Закон про управління інформаційною безпекою федерального уряду).

Розглянемо приклад FISMA. Це закон США, який вимагає від федеральних агентств розробляти, документувати та впроваджувати програму інформаційної безпеки на рівні всього агентства[5].

Мета FISMA: забезпечити захист інформації та інформаційних систем, які підтримують операції та активи агентства.

Вимоги FISMA: агентства повинні забезпечувати захист інформації відповідно до ризику та масштабу шкоди, яка може виникнути в результаті несанкціонованого доступу, використання, розголошення, порушення, модифікації або знищення.

Застосування: FISMA стосується федеральних агентств, підрядників або інших джерел, які забезпечують інформаційну безпеку для інформації та інформаційних систем, що підтримують операції та активи агентства.

Стандарти та керівництва NIST: агентства повинні дотримуватися стандартів інформаційної безпеки та керівництв, розроблених Національним інститутом стандартів та технологій.

Тому, FISMA є дуже важливим законом для підтримки високих стандартів інформаційної безпеки у федеральному уряді США та заохочує агентства впроваджувати надійні програми управління ризиками та регулярно оцінювати їх ефективність.

Ще одним важливим аспектом є дотримання вимог законодавства щодо конфіденційності даних та повідомлення про інциденти, пов'язані з витоком конфіденційної інформації. Наприклад, у Європейському Союзі діє Загальний регламент про захист даних (GDPR), який встановлює суворі вимоги до повідомлення про інциденти, пов'язані з витоком персональних даних, протягом 72 годин після виявлення інциденту.

Окрім дотримання нормативних вимог, важливо також враховувати найкращі практики та рекомендації галузевих організацій та спільнот.

Наприклад, FIRST (The Forum of Incident Response and Security Teams, або Форум команд реагування на інциденти інформаційної безпеки) — це міжнародна спільнота, яка налічує понад 600 команд реагування. Спільнота була заснована у 1990 році і з того часу виросла до глобальної мережі, яка включає сотні організацій-членів з різних секторів, включаючи урядові агентства, приватні компанії, наукові установи та некомерційні організації [6]. Метою є підвищення ефективності та координації в реагуванні на інциденти інформаційної безпеки по всьому світу.

Основні завдання та діяльність FIRST включають:

- Обмін інформацією: Забезпечення платформи для обміну технічною інформацією, попередженнями про нові загрози та методи їх нейтралізації.
- Навчання та тренінги: Організація конференцій, семінарів, тренінгів та інших заходів для підвищення кваліфікації фахівців.
- Розробка стандартів: Вироблення рекомендацій та стандартів у галузі реагування на інциденти інформаційної безпеки.
- Сприяння співпраці: Створення умов для тісної співпраці між членами організації, а також з іншими відповідними організаціями та установами.
- Підтримка досліджень: Сприяння дослідженням у сфері кібербезпеки для виявлення нових загроз та розробки методів їх запобігання.

Учасники FIRST також отримують доступ до різних ресурсів, включаючи інформаційні бюлетені, бази даних про загрози та спеціалізовані інструменти для реагування на інциденти.

Інші організації, такі як ISACA, ISC² та (ISC)², також пропонують сертифікації, навчальні програми та ресурси, пов'язані з управлінням інцидентами.

Окрім міжнародних стандартів, в Україні також діють національні нормативні документи, що регулюють питання управління інцидентами інформаційної безпеки.

Одним з ключових документів є НД ТЗІ 3.7-003-2005 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" (рис. 1.3). Цей нормативний документ визначає загальні вимоги до процесу створення комплексної системи захисту інформації, включаючи етапи виявлення, реагування та усунення інцидентів інформаційної безпеки [7].

Основні вимоги та положення, визначені НД ТЗІ 3.7-003-2005, включають:

- Організація процесу створення КСЗІ - визначення організаційних заходів щодо створення та призначення відповідальних осіб за розробку та впровадження КСЗІ.

- Аналіз загроз та вразливостей - проведення аналізу можливих загроз для ІТС та визначення вразливих місць у системі, що можуть бути використані для несанкціонованого доступу або інших видів атак.

- Розробка та впровадження політик безпеки - розробка політик і процедур щодо захисту інформації та впровадження механізмів контролю за дотриманням цих політик.

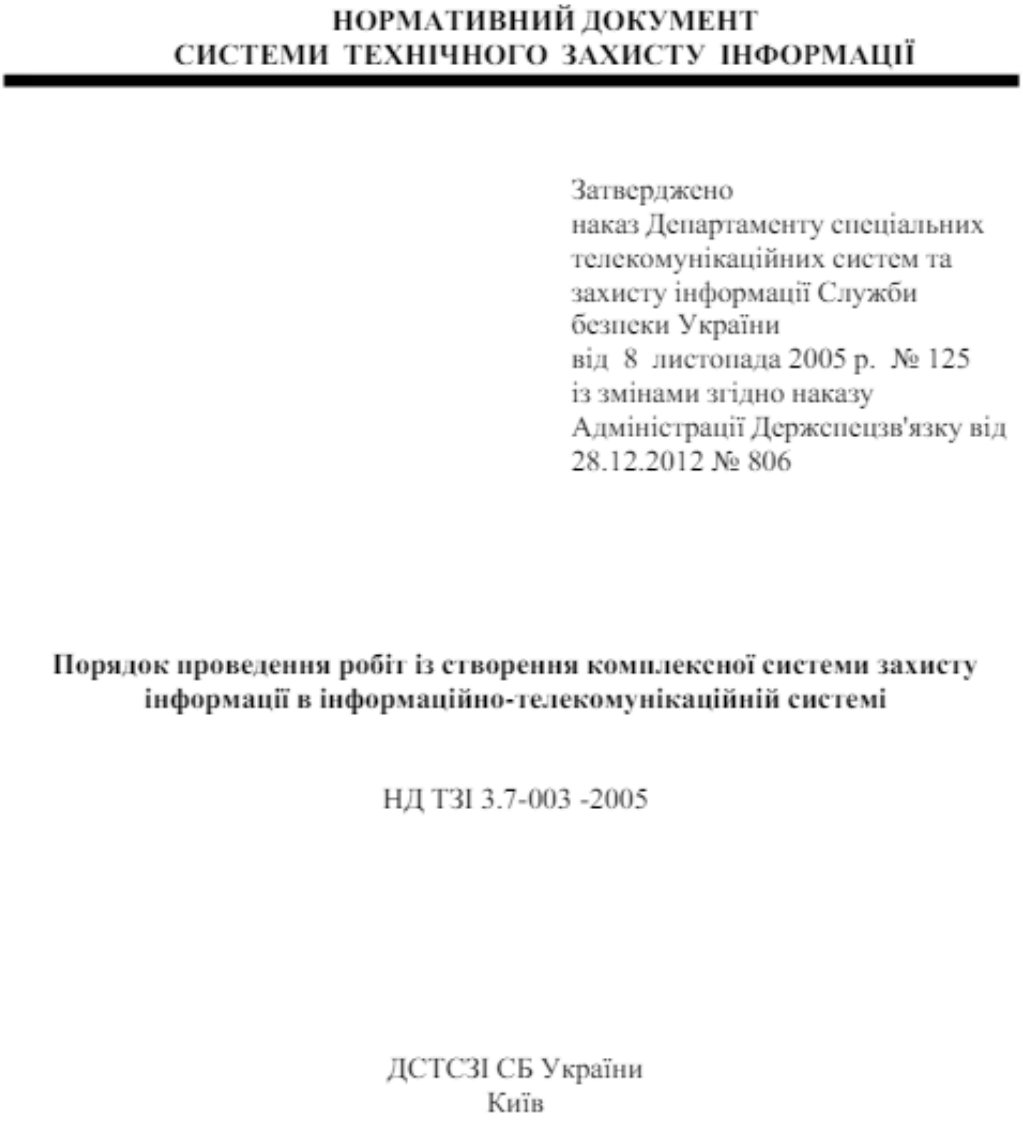
- Технічний захист інформації (ТЗІ) - використання криптографічних засобів для захисту інформації та забезпечення цілісності та конфіденційності даних через застосування відповідних технічних засобів.

- Фізичний захист інформації - встановлення контролю доступу до приміщень, де зберігається або обробляється інформація та вживання заходів щодо захисту інформації від фізичного втручання або пошкодження.

- Моніторинг та аудит системи - регулярний моніторинг стану безпеки ІТС та проведення аудиту для виявлення порушень та несанкціонованих дій.

- Реагування на інциденти безпеки - впровадження процедур для виявлення, реєстрації та реагування на інциденти інформаційної безпеки та аналіз інцидентів та вжиття заходів щодо їхнього запобігання в майбутньому.

- Навчання персоналу - проведення навчання для співробітників щодо правил і процедур захисту інформації та підвищення обізнаності про загрози та методи їхнього запобігання.



НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
наказ Департаменту спеціальних
телекомунікаційних систем та
захисту інформації Служби
безпеки України
від 8 листопада 2005 р. № 125
із змінами згідно наказу
Адміністрації Держспецзв'язку від
28.12.2012 № 806

Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

НД ТЗІ 3.7-003 -2005

ДСТСЗІ СБ України
Київ

Рис. 1.3. Обкладинка НД ТЗІ 3.7-003-2005

Важливим національним стандартом є ДСТУ ISO/IEC 27035:2018 "Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки" (рис. 1.4). Цей стандарт є гармонізованим з міжнародним стандартом ISO/IEC 27035 і встановлює вимоги до процесу управління інцидентами інформаційної безпеки в організаціях України.

ДСТУ ISO/IEC 27035:2018 складається з двох частин:

Частина 1. Принципи керування інцидентами, включає[1]:

- Основні концепції та принципи управління інцидентами інформаційної безпеки.
- Цілі управління інцидентами.
- Переваги структурованого підходу.
- Адаптивність.
- Фази, які включають планування та підготовку, виявлення та звітність, оцінку та рішення, реагування та вивчення уроків.

Частина 2. Настанова щодо планування та підготовки до реагування на інциденти, включає[8]:

- Політику управління інцидентами інформаційної безпеки.
- Оновлення політики інформаційної безпеки.
- Створення плану управління інцидентами інформаційної безпеки.
- Встановлення команди реагування на інциденти.

Ці дві частини разом надають структурований підхід до підготовки, виявлення, звітування, оцінки, реагування на інциденти та застосування вивчених уроків.

Рис. 1.4. ДСТУ ISO/IEC 27035:2018 та його частини

Окрім зазначених вище нормативних документів, в Україні діють також інші стандарти та настанови, що стосуються питань управління інцидентами інформаційної безпеки. Наприклад, ДСТУ 3335.1-96 "Захист інформації. Об'єкти цивільного призначення. Порядок створення комплексної системи захисту інформації" та ДСТУ 4145-2002 "Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка".

Дотримання національних стандартів та нормативних документів є обов'язковим для державних органів влади, підприємств та організацій, що працюють з інформацією, що підлягає захисту згідно з законодавством України. Важливо зазначити, що вимоги до управління інцидентами інформаційної безпеки постійно оновлюються та вдосконалюються відповідно до змін у технологіях, ризиках та загрозах. Тому організації повинні регулярно переглядати та оновлювати свої політики, процедури та плани реагування на інциденти, враховуючи як міжнародні, так і національні стандарти та нормативні вимоги.

Крім того, важливо забезпечити належне навчання та підвищення кваліфікації персоналу, задіяного в процесах управління інцидентами інформаційної безпеки. Це дозволить підвищити ефективність реагування на інциденти та мінімізувати їх наслідки.

Підсумовуючи, дотримання нормативних вимог та стандартів, як міжнародних, так і національних, є необхідною умовою для забезпечення

ефективного управління інцидентами інформаційної безпеки в організаціях України. Однак для досягнення максимальної ефективності необхідно також враховувати галузеві рекомендації, найкращі практики та постійно вдосконалювати процеси управління інцидентами відповідно до змін у середовищі інформаційної безпеки.

Важливо пам'ятати, що нормативні вимоги та стандарти є лише базовими вимогами, а ефективне управління інцидентами інформаційної безпеки вимагає комплексного підходу та постійного вдосконалення процесів з урахуванням специфіки організації, галузі та зовнішнього середовища.

Крім того, слід регулярно переглядати та оновлювати політики, процедури та плани реагування на інциденти, враховуючи зміни в технологіях, ризиках та загрозах інформаційній безпеці. Це допоможе забезпечити актуальність та ефективність процесів управління інцидентами інформаційної безпеки. Підсумовуючи, дотримання нормативних вимог та стандартів є необхідною умовою для забезпечення ефективного управління інцидентами інформаційної безпеки в організації. Однак не слід обмежуватися лише цими вимогами, а також враховувати галузеві рекомендації, найкращі практики та постійно вдосконалювати процеси управління інцидентами відповідно до змін у середовищі інформаційної безпеки.

Висновки до розділу 1

У цьому розділі розглянуто теоретичні аспекти управління інцидентами в інформаційній безпеці, їх місце в загальній системі безпеки, а також вимоги нормативних документів до цих процесів. Ефективне управління інцидентами потребує системного підходу, який включає кваліфікований персонал, технології для виявлення та реагування на інциденти, а також чіткі процедури та плани дій. Цей процес пов'язаний з оцінкою ризиків, управлінням безперервністю бізнесу, управлінням змінами та забезпеченням відповідності нормативним вимогам.

Основні вимоги до управління інцидентами інформаційної безпеки викладені в стандартах ISO/IEC 27001, ISO/IEC 27035, NIST SP 800-61, SANS

Incident Handler's Handbook та інших. Ці документи описують ключові етапи процесу управління інцидентами, включаючи створення політик, процедур і планів реагування, формування групи реагування, навчання персоналу, документування інцидентів, звітність та проведення аналізу після інцидентів. Важливо також враховувати галузеві нормативні вимоги та рекомендації, а також законодавчі вимоги щодо конфіденційності даних та повідомлення про інциденти.

Дотримання нормативних вимог та стандартів є необхідною умовою для ефективного управління інцидентами інформаційної безпеки, проте організації не повинні обмежуватися лише цими вимогами. Вони мають враховувати специфіку своєї діяльності, галузі та зовнішнього середовища, а також постійно вдосконалювати процеси управління інцидентами для надійного захисту інформаційних активів.

РОЗДІЛ 2. АНАЛІЗ СУЧАСНИХ МЕТОДІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В цьому розділі проаналізуємо сучасні методи управління інцидентами інформаційної безпеки. Розглянемо досвід використання сучасних методів у різних організаціях та галузях.

2.1. Огляд сучасних методів управління інцидентами інформаційної безпеки.

Управління інцидентами інформаційної безпеки є критично важливим аспектом забезпечення безперервності бізнесу та захисту конфіденційної інформації організацій. Сучасні методи управління інцидентами розвиваються з урахуванням постійно змінюваного ландшафту загроз інформаційній безпеці, нових технологій та вимог нормативних актів.

1. Методика від NIST (**NIST** – це Національний інститут стандартів та технологій США) (див. рис 2.1.). Методика управління інцидентами інформаційної безпеки NIST, описана в документі NIST SP 800-61 Rev. 2, є одним з найвпливовіших стандартів у цій сфері. [4]

Ініціація створення цього керівництва походила від адміністрації президента США, тому що державні органи влади та управління перебувають під постійними кібератаками. Потрібно було розробити єдиний посібник для фахівців із кібербезпеки та керівників, щоб вони могли використовувати загальну термінологію. У результаті вийшов так званий рамковий документ, який формує загальну понятійну базу. Він був перекладений багатьма мовами, зокрема українською. Стандарт використовується для забезпечення надійного кіберзахисту на підприємствах критичної інфраструктури та в державних органах по всьому світу. Комерційні підприємства та організації також

застосовують NIST Cybersecurity Framework як основний орієнтир для побудови бездоганної системи кібербезпеки.

В основі платформи NIST Cybersecurity Framework лежить ієрархічна структура основних підходів до Інформаційної безпеки (ІБ).

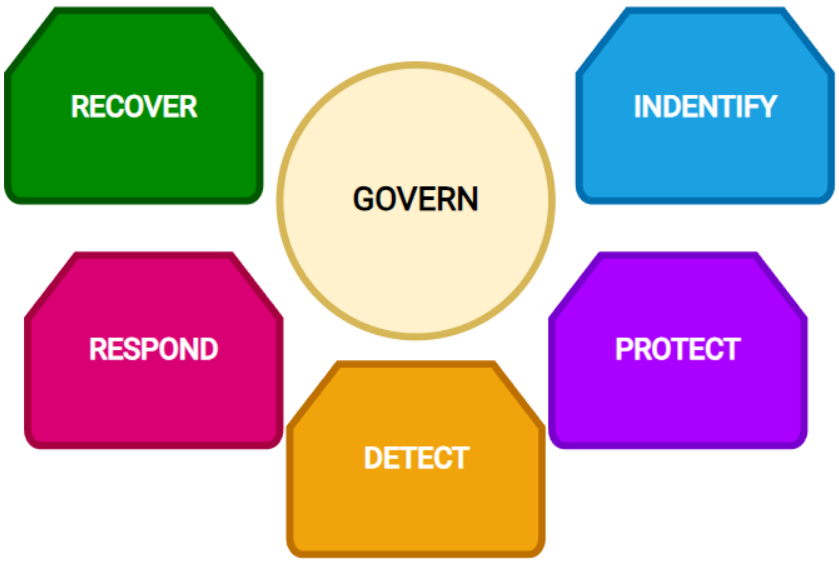


Рис 2.1. Компоненти NIST

1. Identify (Ідентифікація) - розробка організаційної програми кібербезпеки для виявлення, спілкування та управління ризиками кіберзагроз внутрішніми та зовнішніми для систем, активів, даних та можливостей.

2. Protect (Захист) - розробка та впровадження належних заходів безпеки для забезпечення доставки критичних інфраструктурних послуг.

3. Detect (Виявлення) - розробка та впровадження відповідних заходів для своєчасного виявлення подій кібербезпеки.

4. Respond (Реагування) - розробка та впровадження відповідних заходів для вжиття дій щодо події кібербезпеки.

5. Recover (Відновлення) - розробка та впровадження відповідних заходів для підтримки планів стійкості та відновлення будь-яких можливостей чи послуг, які були порушені внаслідок події кібербезпеки.

6. Govern (Управління) - полягає у визначенні пріоритетних заходів та

управлінні рішеннями в усіх функціях для забезпечення кібербезпеки.

Ця методологія допомагає організаціям застосувати структурований підхід до управління ризиками кібербезпеки та захистити свої критичні інформаційні системи та активи.

На етапі підготовки організація створює політики, процедури, плани реагування на інциденти та формує команду реагування. На етапі виявлення та аналізу відбувається моніторинг систем, збір даних про інцидент, його первинний аналіз та класифікація.

2. Методика від компанії SANS (SysAdmin, Audit, Network, Security) Методика управління інцидентами SANS [9], описана в Посібнику з реагування на інциденти SANS, є ще одним широковідомим та визнаним стандартом. Вона включає шість основних етапів:

Підготовка (Preparation): Організації проводять огляд своєї політики безпеки, що зазвичай включає оцінку ризиків для виявлення вразливостей, чутливих активів та областей фокусування у випадку інцидентів безпеки На етапі утримання вживаються заходи для обмеження поширення інциденту та збереження доказів.

Ідентифікація (Identification): Визначення та аналіз інцидентів, щоб зрозуміти їх природу та вплив

Стримування (Containment): Застосування заходів для запобігання поширенню інциденту.

Ліквідація (Eradication): Видалення загрози та усунення причин інциденту

Відновлення (Recovery): Відновлення систем та процесів до нормального стану.

Уроки, що були засвоєні (Lessons Learned): Аналіз інциденту після його закриття для виявлення можливостей поліпшення та запобігання подібним інцидентам у майбутньому.

3. Методика від CERT/CC [10] (Координаційний центр реагування на комп’ютерні надзвичайні ситуації) розроблена однойменним Центром

реагування на комп'ютерні надзвичайні ситуації при Університеті Карнегі-Меллона.

На підготовчому етапі створюються політики, процедури, плани реагування та формується команда реагування. Виявлення передбачає моніторинг систем та ідентифікацію ознак інцидентів. Класифікація інцидентів та встановлення пріоритетів полягає в аналізі виявлених випадків та визначенні черговості реагування.

Етап реагування включає безпосередні дії для усунення інциденту та відновлення роботи систем.

На завершальному етапі вдосконалення проводиться аналіз інциденту і коригування процедур для більш ефективного управління в майбутньому. Схема етапів зображена на рис. 2.2.

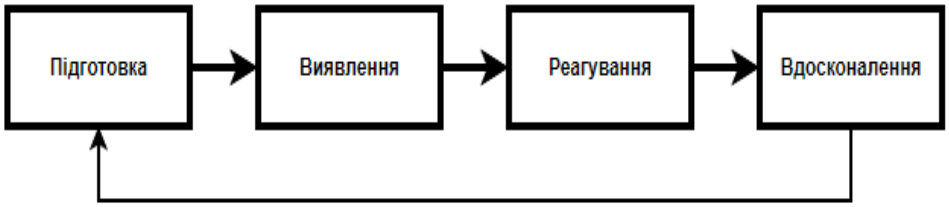


Рис 2.2. Схема етапів CERT/CC

На етапі підготовки створюються політики, процедури, плани реагування та формується команда реагування. Виявлення полягає у моніторингу систем та виявленні ознак інцидентів. Під час інциденту аналізуються, класифікуються та встановлюються пріоритети реагування. На етапі реагування вживаються заходи для усунення інциденту та відновлення нормальної роботи систем. Нарешті, на етапі вдосконалення проводиться аналіз інциденту, коригуються процедури та плани для запобігання подібним інцидентам у майбутньому.

4. Методика відповідно до вимог стандарту ISO/IEC 27035 пропонує загальну структуру та принципи управління інцидентами інформаційної безпеки. Вона базується на циклічному процесі постійного вдосконалення, який

складається з п'яти основних етапів: планування та підготовки, виявлення та повідомлення, оцінки інцидентів та прийняття рішень, реагування та вдосконалення. Схема циклічного процесу згідно цієї методики наведена на рис. 2.3

На етапі планування та підготовки створюються політики, процедури, плани реагування та формується команда реагування. Виявлення та повідомлення полягає у моніторингу систем, ідентифікації інцидентів та інформуванні зацікавлених сторін. Під час оцінки інцидентів та прийняття рішень відбувається аналіз, класифікація випадків та визначення необхідних дій. Реагування включає безпосередні заходи для усунення інциденту і відновлення роботи систем. Вдосконалення передбачає аналіз інциденту та внесення змін для покращення процесу управління.

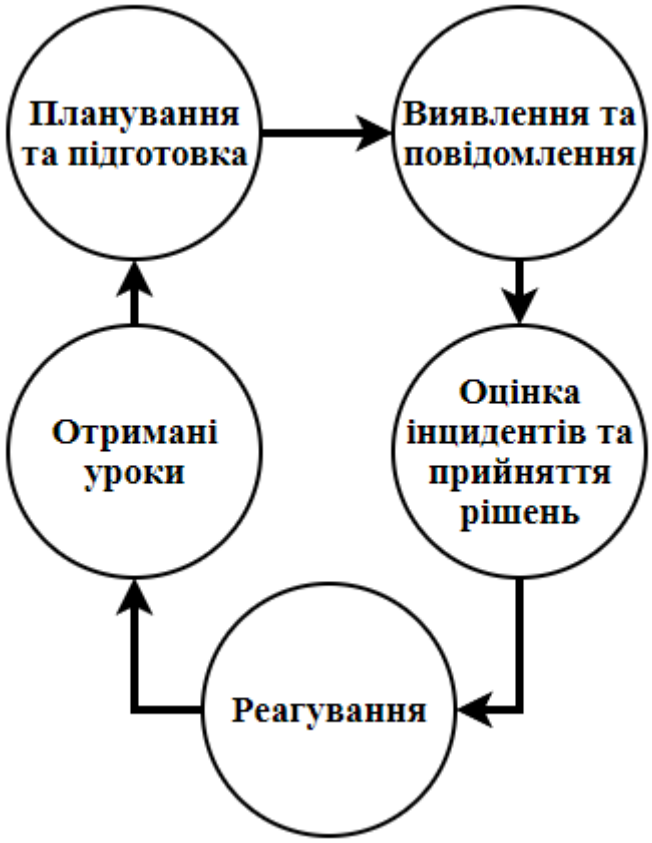


Рис 2.3.Схема методики від ISO/IEC 27035

1. Plan & Prepare (Планування та підготовка) - на цьому етапі створюються політики, процедури, плани реагування на інциденти та формується команда реагування.

2. Identify, Detect, & Report (Виявлення та повідомлення) - полягає у моніторингу систем, ідентифікації інцидентів інформаційної безпеки та інформуванні відповідних зацікавлених сторін.

3. Assessment & Decision (Оцінка інцидентів та прийняття рішень) - проводиться аналіз та класифікація виявлених інцидентів, а також визначаються необхідні дії для реагування.

4. Responses (Реагування) - вживаються безпосередні заходи для усунення інциденту та відновлення нормальної роботи систем.

5. Lessons Learnt (Отримані уроки) - здійснюється аналіз інциденту, коригуються процедури та плани для запобігання подібним інцидентам у майбутньому на основі отриманого досвіду.

Стрілки між етапами вказують на циклічний та ітераційний характер процесу управління інцидентами за цією методикою. Результати кожного етапу використовуються для вдосконалення наступних ітерацій циклу.

5. Методика від ITIL [11] (Бібліотека інфраструктури інформаційних технологій) - ця бібліотека містить рекомендації, щодо надання якісних IT-послуг, процесів і компонентів, необхідних для їх підтримки

Ключові принципи ITIL:

- Просування сучасних знань і обмін досвідом в IT-галузі.
- Організація управління IT-послугами у вигляді сукупності процесів, що дозволяє уніфікувати багато аспектів діяльності різних постачальників IT-послуг.
- Планомірна і поетапна трансформація (без різкого «зламу») вже існуючих процесів Вашого IT-підрозділу.

Мета ITIL - дати рекомендації для побудови IT-процесів таким чином, щоб актуальні IT-послуги надавалися Замовнику оптимальним чином. Для цього

пропонується сформувати перелік (каталог) послуги IT-підрозділу і організувати відповідні групи IT-процесів, що керують життєвим циклом послуг зображені на рис. 2.4.

Рис 2.4. Компоненти послуг від ITIL

- Service Strategy - Побудова стратегії
- Service Design - Проектування послуги
- Service Transition - Перетворення (впровадження) послуги
- Service Operation - Експлуатація послуги
- Continual Service Improvement - Безперервне поліпшення послуги

Усі ці методики мають певні спільні риси, такі як структурований підхід до управління інцидентами, акцент на підготовку, виявлення, реагування та вдосконалення процесів. Проте, кожна з них має свої особливості та може бути більш доцільною в різних ситуаціях, галузях чи організаціях. Організації можуть адаптувати та комбінувати ці методики відповідно до своїх потреб та специфіки.

Окрім загальних методик, існують також спеціалізовані підходи до управління інцидентами інформаційної безпеки в певних галузях або для певних типів інцидентів, наприклад, для реагування на інциденти, пов'язані з витоками даних, кіберзлочинами чи атаками на критичну інфраструктуру.

2.2. Аналіз досвіду використання методів управління інцидентами

Ефективне впровадження та використання методів управління інцидентами інформаційної безпеки є критично важливим для забезпечення безперервності бізнесу та захисту цінних інформаційних активів організацій.

Фінансова сфера є однією з галузей, де управління інцидентами інформаційної безпеки має вирішальне значення. Через високий рівень конфіденційності інформації та суворі нормативні вимоги, фінансові установи зобов'язані мати ефективні процеси реагування на інциденти. Багато банків та страхових компаній успішно впровадили методику NIST або галузевий стандарт FFIEC (Federal Financial Institutions Examination Council), ґрунтується на рекомендаціях NIST.

Наприклад, один з провідних американських банків використовує комбінацію методик NIST та SANS для управління інцидентами інформаційної безпеки. Вони мають спеціалізовану команду реагування на інциденти (CIRT), яка відповідає за виявлення, аналіз, реагування та відновлення після інцидентів. Ця команда тісно співпрацює з підрозділами інформаційної безпеки, IT-операцій та бізнес-підрозділами банку для забезпечення ефективного реагування та мінімізації впливу інцидентів.[12]

У галузі охорони здоров'я управління інцидентами інформаційної безпеки набуває особливої важливості через необхідність захисту конфіденційних медичних даних пацієнтів. Багато медичних установ впроваджують методики, засновані на стандартах HIPAA (Health Insurance Portability and Accountability Act) та NIST.

Ця лікарняна мережа має централізовану команду реагування на інциденти, яка відповідає за моніторинг систем, аналіз інцидентів та координацію дій з підрозділами IT та інформаційної безпеки в кожній лікарні. Вони також активно співпрацюють з галузевими організаціями та державними органами для обміну інформацією про загрози та найкращими практиками реагування на інциденти.

У галузі виробництва та енергетики методи управління інцидентами часто пов'язані із захистом критичної інфраструктури та забезпеченням безперервності операцій.[29, 33, 39] Багато промислових підприємств та енергетичних компаній використовують стандарти, такі як NIST або IEC 62443 (серія стандартів безпеки промислових мереж і систем автоматизації).

Наприклад, одна з великих нафтогазових компаній успішно впровадила методику управління інцидентами, засновану на IEC 62443 та NIST. Вони мають спеціалізований центр реагування на інциденти, який відповідає за моніторинг та захист критичних систем управління та автоматизації виробництва. Цей центр тісно співпрацює з підрозділами IT, операційними підрозділами та постачальниками обладнання для забезпечення швидкого реагування на інциденти та мінімізації їх впливу на виробничі процеси.[13]

У державному секторі управління інцидентами інформаційної безпеки є особливо важливим через необхідність захисту конфіденційної інформації, пов'язаної з національною безпекою та державними послугами. Багато урядових організацій використовують стандарти NIST, FISMA (Federal Information Security Management Act) або спеціалізовані методики, розроблені для конкретних галузей.

Наприклад, одне з міністерств США використовує гібридну методику, що поєднує елементи NIST, SANS та CERT/CC, для управління інцидентами інформаційної безпеки. Вони мають централізований центр реагування на інциденти, який відповідає за моніторинг систем, аналіз інцидентів та координацію дій з різними підрозділами міністерства та зовнішніми партнерами.

Важливим аспектом їхнього підходу є тісна співпраця з іншими урядовими агентствами та організаціями з питань кібербезпеки, такими як US-CERT (United

States Computer Emergency Readiness Team) та CISA (Cybersecurity and Infrastructure Security Agency). Це дозволяє обмінюватися інформацією про загрози, індикатори компрометації та ефективні методи реагування на інциденти.

У сфері телекомунікацій та IT-послуг методи управління інцидентами часто базуються на рекомендаціях ITIL та стандартах, таких як ISO 27035. Багато провайдерів послуг мають власні спеціалізовані команди реагування на інциденти, які відповідають за моніторинг, аналіз та реагування на інциденти, що впливають на наданні послуги клієнтам. Наприклад, одна з великих телекомунікаційних компаній використовує методику ITIL для управління інцидентами інформаційної безпеки. Вони мають централізовану службу підтримки, яка відповідає за реєстрацію та первинну класифікацію інцидентів, а також спеціалізовану команду реагування на інциденти, яка займається більш складними випадками.

Важливими факторами є наявність кваліфікованого персоналу, ефективні технології для виявлення та реагування на інциденти, чіткі процедури та плани дій.

Одним з ключових аспектів ефективного управління інцидентами інформаційної безпеки є налагоджена співпраця та комунікація між різними зацікавленими сторонами. Команда реагування на інциденти повинна тісно взаємодіяти з підрозділами IT, інформаційної безпеки, юридичним відділом, керівництвом організації та, в деяких випадках, зовнішніми партнерами та органами влади.[14]

Ефективна комунікація забезпечує швидкий обмін критично важливою інформацією, координацію дій та прийняття рішень у відповідь на інциденти. Важливо мати чіткі канали комунікації та протоколи звітності, щоб забезпечити своєчасне інформування відповідальних осіб про інциденти та їх подробиці. Крім того, регулярні навчання та тренування є життєво важливими для підтримки готовності команд реагування на інциденти. Проведення симуляцій інцидентів, практичних вправ та навчальних сценаріїв допомагає команді

відпрацювати процедури реагування, визначити можливі прогалини та вдосконалити свої навички. Табл. 2.1., узагальнює використання методів управління інцидентами інформаційної безпеки в різних галузях, наведених у тексті

Таблиця 2.1.

Використання методів управління інцидентами інформаційної безпеки в різних галузях

Галузь	**Компанія/Організація**	**Використовувані методики**	**Короткий опис**
Фінансова сфера	Провідний американський банк	NIST, SANS, FFIEC	Спеціалізована команда реагування (CIRT) використовує комбінацію методик для ефективного реагування та мінімізації впливу інцидентів.
Охорона здоров'я	Лікарняна мережа	HIPAA, NIST	Централізована команда реагування співпрацює з підрозділами IT та інформаційної безпеки в кожній лікарні. Обмін інформацією з галузевими організаціями.
Виробництво, енергетика	Нафтогазова компанія	IEC 62443, NIST	Спеціалізований центр реагування захищає критичні системи управління та автоматизації виробництва. Тісна співпраця з підрозділами IT і постачальниками обладнання.
Державний сектор	Міністерство США	NIST, SANS, CERT/CC	Централізований центр реагування співпрацює з різними підрозділами міністерства та зовнішніми партнерами. Обмін інформацією з US-CERT, CISA.

Продовження таблиці 2.1.

Галузь	Компанія/Організація	Використовувані методики	Короткий опис
Телекомунікації, IT-послуги	Телекомунікаційна компанія	ITIL	Централізована служба підтримки та спеціалізована команда реагування. Тісна співпраця з підрозділами IT-операцій та інформаційної безпеки.

Ще одним ключовим фактором успіху є постійний моніторинг та аналіз тенденцій у сфері кібербезпеки. Це включає відстеження нових загроз, вразливостей та методів атак, а також аналіз інцидентів, що відбулися в організації або в галузі загалом. Такий аналіз дозволяє виявляти моделі та тенденції, що допомагає вдосконалити процеси виявлення та реагування на інциденти. Співпраця з галузевими організаціями, групами з обміну інформацією про загрози (ISAC) та державними органами також є важливою складовою успіху. Обмін інформацією про інциденти, індикатори компрометації та ефективні методи реагування допомагає організаціям краще підготуватися до майбутніх інцидентів та вчитися на досвіді інших.

Нарешті, регулярний аудит та перегляд процесів управління інцидентами є необхідним для забезпечення їх актуальності та ефективності. Технології, загрози та бізнес-вимоги постійно змінюються, тому організації повинні регулярно переглядати свої процеси, оновлювати плани реагування та впроваджувати необхідні поліпшення. Загалом, успішне управління інцидентами інформаційної безпеки вимагає комплексного підходу, який охоплює підготовлену команду, ефективні технології, чіткі процедури, тісну співпрацю та постійне вдосконалення. Організації, які приділяють належну увагу цим аспектам, матимуть кращі шанси швидко реагувати на інциденти, мінімізувати їх вплив та захистити свої цінні активи.

2.3. Проблеми і виклики сучасних методів управління інцидентами

Незважаючи на наявність численних методик та стандартів, управління інцидентами інформаційної безпеки продовжує залишатися складним завданням для багатьох організацій. Існує ряд проблем і викликів, з якими стикаються організації під час впровадження та використання сучасних методів управління інцидентами.

Перш за все, сучасне середовище інформаційних технологій характеризується високим рівнем складності та різноманітністю загроз інформаційній безпеці. Організації повинні захищати численні системи, програми, мережі та пристрої, які постійно змінюються та оновлюються. Крім того, вони стикаються з широким спектром загроз, таких як кібератаки, шкідливе програмне забезпечення, витоки даних, людський фактор та ін. Ця складність створює значні труднощі для виявлення, аналізу та реагування на інциденти. Команди реагування на інциденти повинні мати глибокі знання різноманітних технологій, загроз та методів атак, а також ефективні інструменти для моніторингу та аналізу. Необхідність постійного відстеження змін та адаптації процесів управління інцидентами вимагає значних ресурсів та зусиль.

Однією з основних проблем є брак кваліфікованого персоналу. Вимоги до навичок та знань персоналу, який займається управлінням інцидентами, є досить високими. Вони повинні мати глибоке розуміння технологій інформаційної безпеки, методів аналізу та реагування, а також відповідний досвід роботи. Проте, на ринку праці існує значний дефіцит таких фахівців, особливо з урахуванням зростаючого попиту на послуги з кібербезпеки. Це призводить до високої конкуренції за таланти та підвищення витрат на залучення та утримання кваліфікованого персоналу. Організації також повинні постійно інвестувати в навчання та професійний розвиток своїх команд реагування на інциденти.[15]

Ще однією проблемою є обмежені ресурси та бюджети. Ефективне управління інцидентами інформаційної безпеки вимагає значних інвестицій у персонал, технології, інфраструктуру та процеси. Однак багато організацій

стикаються з обмеженими бюджетами, які необхідно розподіляти між різними пріоритетами та ініціативами з кібербезпеки. Недостатнє фінансування може призвести до браку необхідних інструментів та технологій для виявлення та реагування на інциденти, а також до недостатньої кількості персоналу в командах реагування, що негативно впливає на ефективність управління інцидентами. Складність координації та співпраці також є значним викликом. Управління інцидентами інформаційної безпеки часто вимагає тісної координації та співпраці між різними підрозділами організації, а іноді й залучення зовнішніх ресурсів. Забезпечення ефективної комунікації та узгодженості дій між усіма зацікавленими сторонами може бути складним завданням, особливо в великих або географічно розподілених організаціях, що може призвести до затримок, конфліктів інтересів або неузгодженості дій.

Крім того, багато організацій повинні дотримуватися численних нормативних вимог та стандартів, пов'язаних з інформаційною безпекою та управлінням інцидентами. Забезпечення відповідності всім застосовним нормативним актам та стандартам може бути складним завданням, особливо для організацій, що працюють у кількох юрисдикціях або галузях. Це вимагає ретельного моніторингу змін у нормативно-правовій базі, адаптації процесів управління інцидентами та постійного документування та звітності.[16]

Аналіз та розслідування інцидентів інформаційної безпеки також можуть становити значні труднощі. У випадках складних або цілеспрямованих атак команди реагування на інциденти повинні мати відповідні інструменти, навички та методології для збору та аналізу різноманітних даних, а також забезпечити належне збереження доказів. Ця складність може призвести до затримок у реагуванні, неповного аналізу інцидентів або втрати важливої інформації.

Нарешті, проблеми з обміном інформацією та розповсюдженням знань також є перешкодою для ефективного управління інцидентами. Ефективне управління інцидентами вимагає своєчасного обміну інформацією про нові загрози, вразливості, індикатори компрометації та методи реагування. Однак часто існують перешкоди для обміну такою інформацією, як всередині

організацій, так і між різними організаціями та галузями, через конкуренцію, конфіденційність даних, юридичні обмеження або відсутність відповідних каналів комунікації. Це може призвести до того, що організації не матимуть актуальної інформації про загрози та ефективні методи реагування, що знижує їхню здатність ефективно управляти інцидентами. Ознайомитися з проблемами та їхнім описом можна у табл. 2.2.

Таким чином, управління інцидентами інформаційної безпеки залишається складним завданням, яке вимагає постійних зусиль з подолання численних проблем та викликів, пов'язаних із складністю середовища, браком ресурсів, координацією та нормативною відповідністю. Організації повинні ретельно планувати та впроваджувати комплексні стратегії управління інцидентами, враховуючи ці проблеми, для забезпечення ефективного захисту своїх інформаційних активів та безперервності бізнесу.

Таблиця 2.2.

Проблема/Виклик	**Опис**
Складність та різноманітність загроз	Сучасне IT-середовище вимагає захисту численних систем та пристроїв від різноманітних. Це створює значні труднощі для виявлення, аналізу та реагування на інциденти.
Брак кваліфікованого персоналу	Високі вимоги до навичок та знань, дефіцит кваліфікованих фахівців, висока конкуренція на ринку праці та необхідність постійних інвестицій в навчання та розвиток.
Обмежені ресурси та бюджети	Недостатнє фінансування обмежує можливості інвестування в необхідні інструменти, технології та персонал для ефективного управління інцидентами.

Продовження таблиці 2.2.

Проблема/Виклик	**Опис**
Координація та співпраця	Необхідність тісної координації між підрозділами організації та зовнішніми ресурсами, особливо у великих або географічно розподілених організаціях, що може призводити до затримок та конфліктів.
Нормативні вимоги та стандарти	Забезпечення відповідності нормативним актам та стандартам, що вимагає постійного моніторингу правової бази, адаптації процесів та документування.
Аналіз та розслідування інцидентів	Потреба у відповідних інструментах, навичках та методологіях для збору та аналізу даних під час складних або цілеспрямованих атак, що може призводити до затримок у реагуванні та втрати важливої інформації.
Обмін інформацією та знаннями	Перешкоди для своєчасного обміну інформацією про загрози та методи реагування через конфіденційність даних, юридичні обмеження та відсутність відповідних каналів комунікації.

2.4. Методичні підходи щодо оцінки ефективності управління інцидентами інформаційної безпеки

Оцінка ефективності процесів управління інцидентами інформаційної безпеки є критично важливою для забезпечення безперервного вдосконалення та адаптації до мінливого середовища загроз. Існує ряд методичних підходів, які можуть бути використані організаціями для вимірювання та аналізу ефективності своїх процесів управління інцидентами.

Одним із основних підходів є використання метрик та ключових показників ефективності (KPI). Ці метрики дозволяють кількісно виміряти різні аспекти

процесів управління інцидентами, такі як середній час виявлення та реагування на інциденти, кількість інцидентів, вартість реагування та відновлення, рівень дотримання встановлених процедур тощо. Регулярний моніторинг та аналіз цих метрик дозволяє виявляти тенденції, проблемні області та можливості для вдосконалення. Регулярні аудити та оцінки відповідності також є важливим інструментом для оцінки ефективності управління інцидентами. Під час аудиту оцінюються різні аспекти процесів управління інцидентами відповідно до стандартів, нормативних вимог або найкращих практик. Це дозволяє виявити недоліки та невідповідності, а також надати рекомендації щодо їх усунення.

Тестування та симуляції інцидентів є ефективним способом оцінки готовності організації до реагування на різні типи інцидентів. Команди реагування на інциденти стикаються із змодельованими ситуаціями, які імітують реальні інциденти. Після проведення тестування аналізуються результати, визначаються сильні та слабкі сторони процесів управління інцидентами та розробляються рекомендації щодо їх вдосконалення. Аналіз повернень на інвестиції (ROI) в процеси управління інцидентами є важливим аспектом для організацій, які прагнуть забезпечити ефективне використання ресурсів. Порівнюючи витрати на реагування на інциденти та впровадження процесів управління інцидентами з потенційними збитками, яких вдалося уникнути, організації можуть оцінити, чи є їхні зусилля економічно виправданими.

Порівняння процесів управління інцидентами організації з галузевими стандартами або практиками інших організацій (бенчмаркінг) може бути корисним для оцінки ефективності та визначення можливостей для вдосконалення. Це дозволяє виявити прогалини та відставання в процесах організації та визначити потенційні шляхи для покращення, орієнтуючись на успішні практики інших організацій або галузеві стандарти. Нарешті, організації можуть залучати зовнішніх експертів або консультантів для оцінки ефективності своїх процесів управління інцидентами. Ці експерти можуть надати неупереджену оцінку, базуючись на своєму досвіді та знаннях галузевих практик

і стандартів. Вони також можуть запропонувати рекомендації щодо вдосконалення процесів та стратегії управління інцидентами.[17]

Ефективна оцінка процесів управління інцидентами часто вимагає комбінування кількох з цих методичних підходів для отримання всебічної картини. Регулярний моніторинг, аналіз даних, аудити, тестування та зовнішні оцінки допоможуть організаціям виявляти слабкі місця, відстежувати прогрес та впроваджувати необхідні вдосконалення для підвищення загальної ефективності управління інцидентами інформаційної безпеки. Одним із ключових викликів у процесі управління інцидентами інформаційної безпеки є своєчасне виявлення та ідентифікація інцидентів. Із зростанням кількості та складності кіберзагроз, а також збільшенням обсягів даних, які потрібно відстежувати, стає дедалі складніше виявляти аномалії та ознаки потенційних інцидентів у великому потоці інформації. Ефективні системи моніторингу та аналітики безпеки відіграють важливу роль у вирішенні цього завдання.

Організації повинні впроваджувати комплексні рішення для збору та аналізу різноманітних даних безпеки, таких як журнали подій, мережевий трафік, дані про вразливості та індикатори компрометації. Системи управління інформацією та подіями безпеки (SIEM) є одним із ключових інструментів для консолідації та аналізу цих даних із різних джерел. Вони допомагають виявляти підозрілі моделі поведінки, відхилення від норми та потенційні загрози, забезпечуючи своєчасне сповіщення команд реагування на інциденти.

Крім того, використання технологій штучного інтелекту та машинного навчання може значно підвищити ефективність виявлення інцидентів. Ці технології можуть аналізувати величезні обсяги даних, виявляти складні моделі та адаптуватися до нових загроз, забезпечуючи більш точне та своєчасне виявлення інцидентів. Однак впровадження таких рішень вимагає значних інвестицій, відповідної інфраструктури та кваліфікованого персоналу.

Після виявлення інциденту наступним важливим кроком є його оцінка та пріоритезація. Команди реагування на інциденти повинні мати чіткі критерії та процедури для визначення рівня серйозності інциденту, потенційного впливу та

необхідних дій для реагування. Це допомагає забезпечити ефективне розподілення ресурсів та зосередження зусиль на найбільш критичних інцидентах.[18]

Під час фази реагування на інцидент ключовим є швидке та скоординоване виконання відповідних дій для мінімізації впливу інциденту та відновлення нормальної роботи систем і процесів. Це може включати ізоляцію уражених систем, блокування шкідливого трафіку, відновлення з резервних копій, усунення вразливостей та впровадження додаткових заходів безпеки. Ефективна координація та комунікація між різними командами та підрозділами в організації є критично важливою для успішного реагування на інциденти.

Після стабілізації ситуації та усунення наслідків інциденту, необхідно провести ретельний аналіз та розслідування для визначення причин, векторів атаки та потенційних наслідків. Це допоможе організаціям зрозуміти слабкі місця в їхніх системах безпеки, відповідно адаптувати стратегії захисту та запобігти повторенню подібних інцидентів у майбутньому.

Обмін інформацією про інциденти та загрози є ще одним важливим аспектом ефективного управління інцидентами. Організації повинні розвивати партнерські відносини та брати участь у спільнотах обміну інформацією для отримання актуальних даних про нові загрози, вразливості та методи реагування. Це допоможе їм швидше виявляти та реагувати на інциденти, а також навчатися на досвіді інших організацій.

Регулярний перегляд та оновлення планів реагування на інциденти, проведення навчань та тренувань, впровадження нових технологій та методологій допоможе організаціям підтримувати високий рівень готовності до майбутніх інцидентів та ефективно реагувати на мінливе середовище кіберзагроз. Організації повинні регулярно проводити комплексні тренінги та навчальні програми для своїх команд реагування на інциденти. Ці програми повинні охоплювати різні аспекти управління інцидентами, такі як виявлення та аналіз інцидентів, методи реагування, збереження доказів, розслідування інцидентів, відновлення після інцидентів та звітування. Важливо також

приділяти увагу розвитку технічних навичок, пов'язаних з конкретними технологіями, інструментами та системами, які використовуються в організації. Симуляції інцидентів та практичні навчання є ефективним способом закріплення знань та відпрацювання навичок в умовах, максимально наближених до реальних ситуацій. Під час таких навчань команди реагування на інциденти можуть відпрацьовувати різні сценарії, вчитися приймати рішення в умовах стресу та тиску, а також координувати свої дії з іншими підрозділами.[19]

Крім внутрішніх навчальних програм, організації також можуть залучати зовнішніх експертів або використовувати професійні сертифікаційні програми для підвищення кваліфікації свого персоналу. Це дозволяє отримати доступ до найновіших знань та практик в галузі управління інцидентами, а також забезпечити визнання компетентності персоналу на галузевому рівні. Ефективне управління знаннями також є важливим аспектом підготовки персоналу. Організації повинні забезпечити наявність централізованих репозиторіїв знань, де зберігається інформація про попередні інциденти, використані методи реагування, уроки, які були отримані, та найкращі практики. Це дозволить новим членам команд реагування на інциденти швидко отримувати доступ до накопиченого досвіду, а також забезпечить збереження інституційної пам'яті у випадку плинності кадрів. У стандарті ISO/IEC 27035 "Інформаційні технології - Методи забезпечення безпеки інформаційних технологій - Управління інцидентами інформаційної безпеки" рекомендується використовувати низку метрик для оцінки ефективності процесів управління інцидентами інформаційної безпеки. Ці метрики можуть включати:

1. Середній час виявлення інциденту (MTTD - Mean Time To Detect)
2. Середній час реагування на інцидент (MTTR - Mean Time To Respond)
3. Середній час відновлення після інциденту (MTTR - Mean Time To Recover)
4. Кількість інцидентів за певний період часу
5. Вартість реагування та відновлення після інцидентів

6. Рівень дотримання встановлених процедур управління інцидентами

На основі цих метрик можуть розраховуватись більш складні формули та показники ефективності, такі як:

1. Ефективність виявлення інцидентів = 1 - (Кількість пропущених інцидентів / Загальна кількість інцидентів)

2. Ефективність реагування = 1 - (MTTR / Цільовий час реагування)

3. Ефективність відновлення = 1 - (MTTR / Цільовий час відновлення)

4. Загальна ефективність управління інцидентами = (Ефективність виявлення + Ефективність реагування + Ефективність відновлення) / 3

Ці формули можуть бути адаптовані та налаштовані відповідно до специфічних вимог та цілей організації.

Схематично алгоритм використання метрик безпеки в процесах оцінки ефективності управління інформаційною безпекою та інцидентами інформаційної безпеки вказаний на рис.2.5

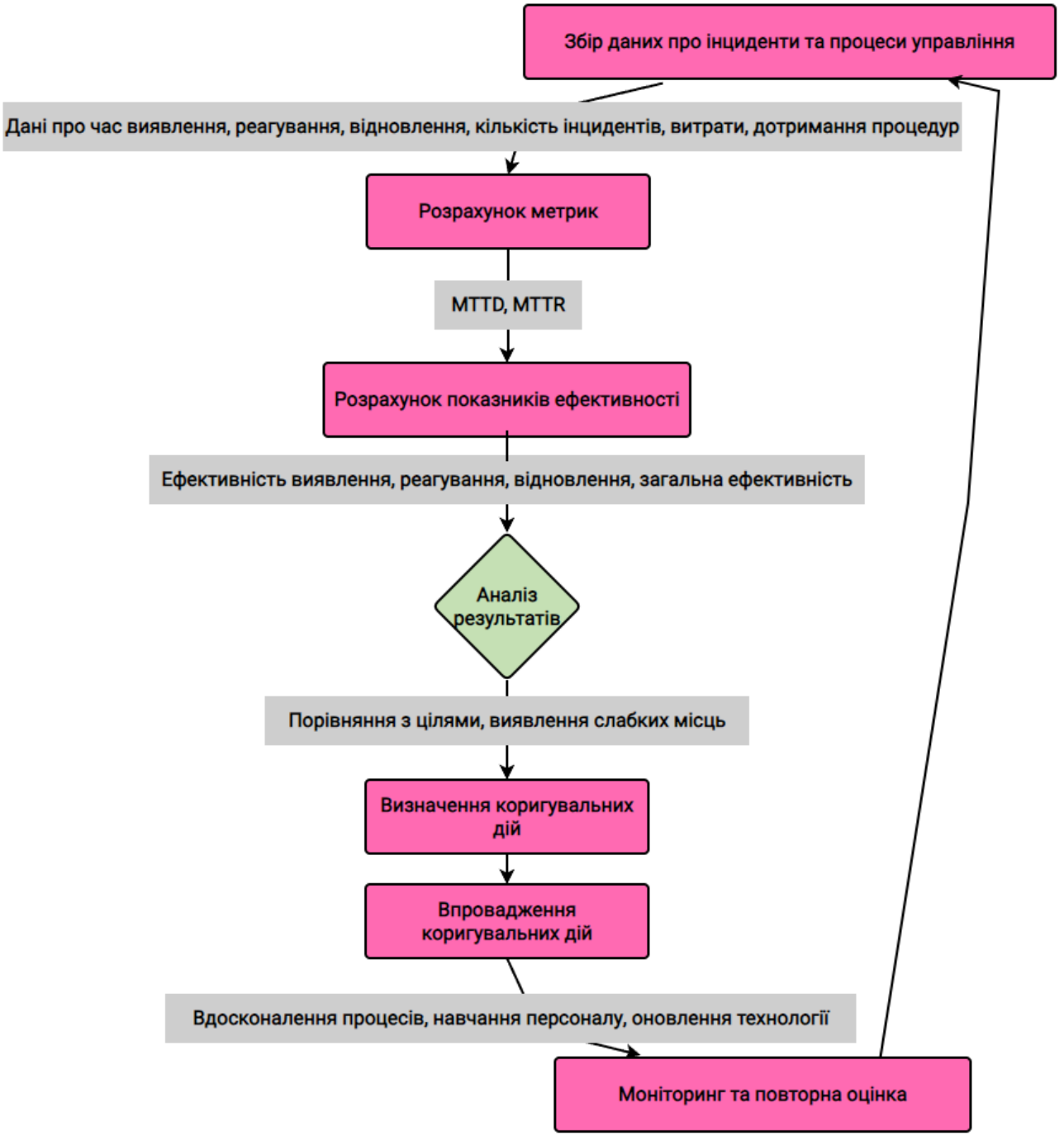


Рис 2.5. Алгоритм використання метрик безпеки в процесах оцінки ефективності управління інформаційною безпекою

Нарешті, організації повинні регулярно оцінювати ефективність своїх програм навчання та підготовки персоналу. Це може включати аналіз результатів симуляцій та практичних навчань, відгуків учасників, а також моніторинг показників ефективності під час реальних інцидентів. На основі цієї оцінки

можна вносити необхідні коригування та вдосконалення в навчальні програми, забезпечуючи постійне підвищення рівня компетентності персоналу.

Таким чином, належна підготовка та навчання персоналу є невід'ємною складовою ефективного управління інцидентами інформаційної безпеки. Інвестуючи в розвиток знань, навичок та компетенцій своїх команд реагування на інциденти, організації зможуть забезпечити швидке та ефективне реагування на інциденти, мінімізуючи їх вплив та захищаючи свої критично важливі активи та операції.

Висновки до розділу 2

Управління інцидентами інформаційної безпеки є критично важливим завданням для забезпечення безперервності бізнесу та захисту цінних інформаційних активів організацій. У цьому розділі було розглянуто сучасні методи та підходи до управління інцидентами, проаналізовано досвід їх використання в різних галузях, а також визначено основні проблеми та виклики, з якими стикаються організації.

Представлено огляд широко використовуваних методик, таких як NIST, SANS, CERT/CC, ISO/IEC 27035, ITIL. Ці методики пропонують структуровані підходи до виявлення, аналізу, реагування та відновлення після інцидентів інформаційної безпеки. Вибір та впровадження відповідної методики залежить від специфіки діяльності організації, нормативних вимог та наявних ресурсів. Аналіз практичного досвіду показав, що ефективне управління інцидентами є складним завданням, яке вимагає системного підходу, залучення відповідних ресурсів та постійного вдосконалення процесів.

Визначено ряд проблем та викликів, з якими стикаються організації під час управління інцидентами, включаючи складність середовища та різноманітність загроз, брак кваліфікованого персоналу, обмежені ресурси та бюджети, складність координації та співпраці, необхідність дотримання нормативних вимог, труднощі з аналізом та розслідуванням інцидентів, а також проблеми з обміном інформацією та розповсюдженням знань.

Для забезпечення ефективного управління інцидентами організації повинні використовувати різноманітні методичні підходи до оцінки та вдосконалення своїх процесів, такі як використання метрик та ключових показників ефективності, регулярні аудити та оцінки відповідності, тестування та симуляції інцидентів, аналіз повернень на інвестиції, бенчмаркінг з галузевими практиками та залучення зовнішніх експертів.

Результати, отримані в цьому розділі, необхідно використати при проведенні подальшого дослідження та отриманні рекомендацій щодо покращення управління інцидентами інформаційної безпеки в організації на конкретному прикладі. Таким чином, будуть виконані задачі дослідження та досягнуті цілі відповідно до назви теми роботи.

Лише комплексний підхід, який поєднує відповідні методики управління інцидентами, ефективні інструменти та технології, кваліфікований персонал та безперервне вдосконалення процесів, може забезпечити високий рівень готовності організації до реагування на інциденти інформаційної безпеки та мінімізувати їх негативний вплив на бізнес.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Проведемо дослідження ефективності управління інцидентами інформаційної безпеки на прикладі конкретної організації. Проаналізуємо поточний стан процесів управління інцидентами за допомогою SWOT-аналізу, виявимо слабкі місця та недоліки. На основі результатів розробимо рекомендації щодо вдосконалення процесів управління інцидентами інформаційної безпеки в організації.

3.1. Аналіз поточного стану управління інцидентами інформаційної безпеки організації за допомогою SWOT-аналізу (на прикладі)

Для ілюстрації практичного застосування методів управління інцидентами інформаційної безпеки та виявлення потенційних областей для вдосконалення, розглянемо приклад організації “SoftTech”. Це велика IT-компанія з кількома офісами в різних країнах, що надає послуги розробки програмного забезпечення, хмарних рішень та консалтингу з інформаційних технологій.

“SoftTech” впровадила комбінований підхід, заснований на методологіях NIST та ITIL, для управління інцидентами інформаційної безпеки. Вони мають централізовану команду реагування на інциденти (CIRT), яка відповідає за виявлення, аналіз, реагування та відновлення після інцидентів безпеки в масштабах всієї компанії.

Процес управління інцидентами складається з таких основних етапів:

1. Виявлення та реєстрація інцидентів
2. Первинний аналіз та класифікація
3. Дослідження та діагностика
4. Реагування та усунення
5. Відновлення та закриття

6. Аналіз після інциденту та вдосконалення процесів

Виявлення інцидентів здійснюється за допомогою комбінації інструментів моніторингу та аналізу журналів, таких як системи виявлення вторгнень (IDS), системи управління інформацією та подіями безпеки (SIEM) та інструменти для моніторингу мереж і хмарних середовищ. Також приймаються повідомлення від користувачів та інших джерел.

Зареєстровані інциденти класифікуються за категоріями та рівнями критичності, а також призначаються відповідні аналітики CIRT для подальшого розслідування. На етапі дослідження та діагностики проводиться детальний аналіз джерел, векторів атаки, впливу та потенційних наслідків інциденту.[20]

На основі результатів аналізу команда CIRT розробляє план реагування та вживає необхідні заходи для усунення інциденту, такі як ізоляція скомпрометованих систем, блокування шкідливого трафіку, відновлення резервних копій даних та оновлення захисних засобів. Паралельно здійснюються дії з відновлення нормальної роботи систем та мінімізації впливу інциденту на бізнес-операції. Після повного усунення інциденту та відновлення систем, CIRT проводить аналіз після інциденту, документує отриманий досвід та розробляє рекомендації для вдосконалення процесів управління інцидентами, політик безпеки та захисних заходів. Організація також має чіткі процедури ескалації та комунікації під час управління інцидентами. Залежно від критичності та впливу інциденту, до процесу залучаються різні зацікавлені сторони, такі як керівництво компанії, юридичний відділ, відділ зв'язків з громадськістю та відповідні підрозділи бізнесу.

Для всебічного аналізу поточного стану управління інцидентами інформаційної безпеки в організації, використаємо метод SWOT-аналізу. Але спочатку визначимо, що таке SWOT-аналіз, для чого його використовують і з чого він складається.

SWOT-аналіз – це аналіз організації, її внутрішніх і зовнішніх факторів, які впливають на роботу і розвиток компанії. Цей аналіз дає чітке уявлення про ситуацію і вказує напрямок розвитку. Це допомагає мінімізувати ризик невдачі.

SWOT є абревіатурою англійських слів Strength (сильні сторони), Weaknesses (слабкі сторони), Opportunities (Можливості) та Threats (загрози), вони ж є чотирма компонентами аналізу.

- Strength (сильні сторони) – це внутрішні характеристики організації, котрі дають перевагу.

- Weaknesses (слабкі сторони) – це внутрішні аспекти, які можуть перешкодити досягненню цілей організації.

- Opportunities (можливості) – це зовнішні фактори, які організація може використовувати для підвищення ефективності своєї діяльності.

- Threats (загрози) – це зовнішні фактори, які можуть негативно вплинути на діяльність організації.

“SoftTech” регулярно проводить аудити всіх підрозділів для отримання їх оцінок ефективності, в тому числі управління інцидентами ІБ.

Припустимо, що після оцінки ефективності управління інцидентами отримали певний обсяг даних для аналізу. На основі даних створимо SWOT-матрицю.

Щоб визначити рівень поточного стану управління інцидентами ІБ організації “SoftTech”, виберемо десяти бальну шкалу, де ефективність інструментів, процесів, роботи і тд. буде визначатись як:

• 0-5 низька;

• 5-8 задовільна;

• 8-10 висока.

Визначимо сильні сторони в табл. 3.1.:

Таблиця 3.1.

Сильні сторони

Номер	Сильна сторона	Оцінка ефективності
1	Впровадження визнаних методологій NIST та ITIL	8
2	Централізована та спеціалізовані команди CIRT	6
3	Сучасні інструменти для виявлення, моніторингу та аналізу інцидентів	5
4	Регулярний аналіз після інцидентів та процес вдосконалення	8

Визначимо слабкі сторони - в табл. 3.2.:

Таблиця 3.2.

Слабкі сторони

Номер	Слабка сторона	Оцінка ефективності
1	Брак ресурсів та перевантаження команди	6
2	Недостатня інтеграція з процесами управління вразливостями та змінами в IT-інфраструктурі	5
3	Обмежений обмін інформацією про загрози та індикатори компрометації всередині та зовні організації	4
4	Відсутність формалізованої програми тестування та навчання персоналу	5

Тепер проведемо аналіз можливостей (табл. 3.3.) і загроз (табл. 3.4.) у наступних матрицях.

Таблиця 3.3.

Матриця можливостей

Номер	Можливість	Імовірність реалізації	Вплив можливостей		
			Слабкий	Помірний	Сильний
1	Розширення команди CIRT та залучення додаткових ресурсів	Середня			+

Продовження таблиці 3.3.

Номер	Можливість	Імовірність реалізації	Вплив можливостей		
			Слабкий	Помірний	Сильний
2	Посилення інтеграції з процесами управління вразливостями, змінами та безперервністю бізнесу.	Середня		+	
3	Налагодження обміну інформацією про загрози з партнерами та галузевими організаціями	Середня		+	
4	Розробка формалізованої програми тестування та навчання для підвищення кваліфікації персоналу.	Високий			+

Таблиця 3.4.

Матриця загроз

Номер	Загроза	Імовірність реалізації	Рівень критичності		
			Слабкий	Помірний	Сильний
1	Зростання кількості та складності інцидентів безпеки	Середня		+	
2	Поява нових видів загроз та векторів атак	Середня		+	
3	Відсутність швидкого реагування на інциденти	Низька			+
4	Недостатня кваліфікація персоналу в управлінні інцидентами	Високий		+	

За допомогою цих таблиць створено матрицю SWOT-аналізу(табл. 3.5.), де Сильні сторони позначені як S, Слабкі сторони – W, Можливості – O, Загрози – T. Щоб визначити вплив загроз і можливостей на сильні і слабкі сторони використовуємо десяти бальну шкалу.

Таблиця 3.5.

Матриця SWOT-аналізу

	T1	T2	T3	T4	O1	O2	O3	O4
S1	5	4	2	3	3	2	8	3
S2	6	7	6	8	8	5	4	7
S3	4	4	3	2	4	7	7	2
S4	4	5	2	2	5	5	8	2
W1	8	7	7	5	9	1	4	5
W2	6	6	4	4	3	9	4	3
W3	4	6	2	2	3	5	9	2
W4	7	8	7	9	4	2	2	9

Далі, на основі SWOT-аналізу матриці, створено таблиці впливу можливостей і загроз на сильні(табл. 3.6.) і слабкі сторони(табл. 3.7.)

Таблиця 3.6.

Вплив на сильні сторони

Сильна сторона	S1	S2	S3	S4
Кількість ймовірність реалізації яких знижує сторона	1	4	0	1
Кількість можливостей реалізації яких сприяє сторона	1	3	2	4

Таблиця 3.7.

Вплив на слабкі сторони

Слабка сторона	W1	W2	W3	W4
Кількість загроз, ймовірність реалізації яких збільшує сторона	3	2	1	4
Кількість можливостей ймовірність реалізації яких сторона знижує	1	1	2	1

Використовуючи SWOT-аналіз поточного стану управління інцидентами інформаційної безпеки в організації “SoftTech” було виявлено ряд сильних сторін, таких як впровадження визнаних методологій, наявність спеціалізованої команди CIRT, використання сучасних інструментів та процесів вдосконалення. Проте, також були визначені потенційні області для вдосконалення, включаючи питання навантаження на команду CIRT, інтеграцію з іншими процесами, обмін інформацією про загрози, тестування та навчання.[21]

Подальші рекомендації щодо вдосконалення процесів управління інцидентами в організації будуть надані в наступному підрозділі враховуючи виявлені сильні сторони та потенційні проблемні зони.

3.2. Рекомендації щодо покращення управління інцидентами управління інформаційної безпеки організації

На основі аналізу поточного стану управління інцидентами інформаційної безпеки в організації “SoftTech”, можемо надати ряд рекомендацій для вдосконалення процесів та підвищення їх ефективності. Ці рекомендації охоплюють різні аспекти, такі як організаційна структура, ресурси, інтеграція процесів, обмін інформацією, автоматизація, тестування та навчання, а також моніторинг та звітність.

Для вирішення проблеми перевантаження та забезпечення своєчасного реагування і відновлення на інциденти, що також підвищить ефективність процесів, організації слід розглянути можливість збільшення чисельності команди CIRT або створення додаткових спеціалізованих команд для окремих типів інцидентів або бізнес-підрозділів. Це дозволить розподілити навантаження та забезпечити більше експертизи в конкретних областях. Також можна розглянути залучення зовнішніх ресурсів або аутсорсинг частини функцій реагування та відновлення на інциденти під час пікових періодів або для конкретних видів інцидентів. Це може бути більш економічно ефективним рішенням, ніж постійне збільшення штату команди CIRT. Для зменшення ризику виникнення інцидентів та підвищення ефективності їх усунення, необхідно забезпечити тісну інтеграцію процесів управління інцидентами з процесами управління вразливостями та змінами в IT-інфраструктурі.[22]

Це може включати:

- Регулярний обмін інформацією про виявлені вразливості та плани їх виправлення між командами CIRT, управління вразливостями та IT-операціями.
- Залучення команди CIRT до процесу затвердження та аналізу ризиків змін в IT-інфраструктурі для виявлення потенційних загроз безпеці.
- Автоматизована координація дій з виправлення вразливостей та внесення змін після інцидентів безпеки.

Для підвищення ефективності та прискорення реагування на інциденти, організації слід впровадити більшу автоматизацію в своїх процесах управління інцидентами. Це може включати:

- Автоматизацію збору та аналізу журналів подій, мережевого трафіку та інших даних для виявлення аномалій та індикаторів інцидентів.
- Використання скриптів та інструментів оркестрації для автоматизації певних дій реагування, таких як ізоляція систем, блокування шкідливого трафіку, розгортання оновлень безпеки тощо.
- Впровадження систем автоматизованого рендіння інцидентів, відстеження статусу та призначення ресурсів.

- Інтеграція автоматизованих процесів реагування з системами управління змінами та конфігураціями для узгодженого внесення змін в IT-середовище під час інцидентів.

Однак, слід забезпечити належний контроль та моніторинг автоматизованих процесів, щоб уникнути неочікуваних наслідків чи порушень безпеки.(див. табл. 3.8.)

Для підвищення готовності команди CIRT та інших залучених підрозділів до ефективного реагування на різноманітні типи інцидентів, організації слід розробити формалізовану програму тестування та навчання.[23]

Ця програма може включати:

- Регулярні тренінги та навчальні курси з різних аспектів управління інцидентами, таких як аналіз загроз, цифрова криміналістика, техніки реагування тощо.
- Симуляції різних сценаріїв інцидентів для практичного відпрацювання навичок реагування та тестування планів дій.
- Моделювання складних цілеспрямованих атак (наприклад, APT) для підготовки до найсерйозніших інцидентів.
- Періодичне тестування технічних засобів та інструментів, що використовуються для виявлення та реагування на інциденти.
- Оцінку результатів тестувань та навчань для виявлення прогалин і удосконалення програми.

Посилення інтеграції з процесами управління ризиками та безперервністю бізнесу. Для забезпечення узгодженості дій під час інцидентів та ефективного відновлення критично важливих бізнес-процесів, організації слід посилити інтеграцію процесів управління інцидентами інформаційної безпеки з процесами управління ризиками та забезпечення безперервності бізнесу.

Це може включати:

- Регулярний обмін інформацією про ризики інформаційної безпеки, оцінки критичності активів та планів безперервності бізнесу між відповідними командами та підрозділами.

- Узгодження критеріїв класифікації та ескалації інцидентів з критеріями оцінки ризиків та пріоритетами відновлення бізнес-процесів.
- Залучення команди CIRT та експертів з інформаційної безпеки до розробки та тестування планів безперервності бізнесу.
- Інтеграцію процесів реагування на інциденти з процедурами активації планів безперервності бізнесу та оперативного реагування на кризові ситуації.

Впровадження цих рекомендацій дозволить організації вдосконалити свої процеси управління інцидентами інформаційної безпеки, підвищити їх ефективність та готовність до реагування на різноманітні типи інцидентів. Це, в свою чергу, зміцнить захист інформаційних активів організації та забезпечить безперервність критично важливих бізнес-операцій.[24]

Таблиця 3.8.

Рекомендації щодо вдосконалення управління інцидентами інформаційної безпеки

Рекомендація	**Очікувані переваги**	**Очікуваний вплив**
Збільшення ресурсів та розподіл навантаження на команду CIRT	- Своєчасне реагування на інциденти - Достатня експертиза для різних типів інцидентів - Зменшення ризику перевантаження команди	- Скорочення середнього часу реагування і відновлення - Збільшення обсягу проаналізованих інцидентів
Впровадження платформи для обміну інформацією про загрози	- Підвищена ситуаційна обізнаність - Ефективніше виявлення та аналіз інцидентів - Обмін досвідом та знаннями всередині організації	- Збільшення кількості виявлених інцидентів - Скорочення середнього часу аналізу інциденту
Формалізована програма тестування та навчання	- Підвищена готовність команди до різних сценаріїв - Виявлення прогалин та вдосконалення навичок - Відпрацювання планів реагування	- Покращення успішності реагування - Зменшення частоти повторних інцидентів

Продовження таблиці 3.8.

Рекомендація	Очікувані переваги	Очікуваний вплив
Інтеграція з управлінням ризиками та безперервністю бізнесу	- Узгодженість дій під час інцидентів - Ефективне відновлення критичних процесів - Зниження ризиків для бізнесу	- Скорочення середнього часу відновлення критичних процесів - Зменшення втрат від інцидентів

Ця таблиця узагальнює ключові рекомендації та очікувані переваги від їх впровадження для вдосконалення процесів управління інцидентами інформаційної безпеки в організації.

Висновки до розділу 3

Було проведено SWOT-аналіз поточного стану управління інцидентами інформаційної безпеки на прикладі організації “SoftTech” та надано рекомендації для вдосконалення процесів управління інцидентами. Аналіз виявив, що загальна ефективність управління інцидентами вимагає поліпшення процесів реагування та відновлення, також компанія впровадила комбінований підхід, заснований на методологіях NIST та ITIL, і має централізовану команду реагування на інциденти (CIRT). Процес управління інцидентами включає виявлення, аналіз, реагування, усунення, відновлення та подальше вдосконалення

Разом з тим, було визначено кілька потенційних областей для надання рекомендацій, таких як брак ресурсів та перевантаження команди CIRT, недостатня інтеграція з процесами управління вразливостями та змінами, обмежений обмін інформацією про загрози, відсутність формалізованої програми тестування та навчання, обмежена інтеграція з процесами управління ризиками та безперервністю бізнесу. На основі виявлених проблемних зон були надані рекомендації щодо вдосконалення процесів управління інцидентами.

ВИСНОВКИ

У кваліфікаційній роботі було проведено ґрунтовне дослідження питань управління інцидентами інформаційної безпеки в сучасних організаціях. Належне управління інцидентами є критично важливим для забезпечення захисту цінних інформаційних активів, підтримання безперервності бізнес-операцій та зменшення негативного впливу інцидентів на репутацію та фінансові показники.

У теоретичній частині роботи було розглянуто основні поняття та концепції управління інцидентами інформаційної безпеки. Визначено поняття інциденту безпеки, його різновиди та потенційний вплив на організацію. Проаналізовано ключові принципи управління інцидентами, такі як профілактика, виявлення, реагування, відновлення та постінцидентний аналіз. Сформульовані основні вимоги та рекомендації різних нормативних документів і стандартів, включаючи NIST SP 800-61, ISO/IEC 27035, SANS, CERT/CC та інші, що забезпечують структуровані підходи до побудови ефективних процесів управління інцидентами.

У практичній частині було представлено огляд широко використовуваних методик управління інцидентами, таких як NIST, SANS, CERT/CC, ISO/IEC 27035, ITIL. Ці методики пропонують комплексні рішення для виявлення, аналізу, реагування, усунення та відновлення після інцидентів безпеки. Водночас, вибір та впровадження відповідної методики залежить від специфіки діяльності організації, нормативних вимог та наявних ресурсів.

Також було проаналізовано практичний досвід управління інцидентами в різних галузях, включаючи фінансову сферу, охорону здоров'я, виробництво, енергетику, державний сектор та IT-послуги. Ці приклади продемонстрували успішне впровадження різноманітних методик з адаптацією до конкретних вимог організацій. Проте, було виявлено ряд проблем та викликів, з якими стикаються організації, зокрема складність середовища та різноманітність загроз, брак кваліфікованого персоналу, обмежені ресурси та бюджети,

складність координації та співпраці, необхідність дотримання нормативних вимог, труднощі з аналізом та розслідуванням інцидентів, а також проблеми з обміном інформацією та розповсюдженням знань.

Для забезпечення ефективного управління інцидентами організації повинні використовувати різноманітні методичні підходи до оцінки та вдосконалення своїх процесів, включаючи використання метрик та ключових показників ефективності, регулярні аудити та оцінки відповідності, тестування та симуляції інцидентів, аналіз повернень на інвестиції, бенчмаркінг з галузевими практиками та залучення зовнішніх експертів.

У межах роботи було проведено детальний аналіз поточного стану управління інцидентами інформаційної безпеки на прикладі організації "SoftTech". Було виявлено, що організація впровадила комбінований підхід, заснований на методологіях NIST та ITIL, має централізовану команду реагування на інциденти (CIRT) та використовує сучасні інструменти для моніторингу та аналізу інцидентів. Водночас, було визначено кілька потенційних областей для вдосконалення, таких як брак ресурсів та перевантаження команди CIRT, недостатня інтеграція з процесами управління вразливостями, недостатня автоматизація процесів реагування, відсутність формалізованої програми тестування та навчання.

На основі виявлених проблемних зон були надані рекомендації щодо вдосконалення процесів управління інцидентами в організації. Ці рекомендації охоплювали збільшення ресурсів та розподіл навантаження на команду CIRT, впровадження централізованої платформи для обміну інформацією про загрози, автоматизацію процесів реагування, розробку програми тестування та навчання, інтеграцію з процесами управління ризиками та безперервністю бізнесу, а також вдосконалення моніторингу та звітності щодо ефективності управління інцидентами.

Регулярний моніторинг, аналіз та безперервне вдосконалення процесів управління інцидентами є критично важливими для підтримання високого рівня готовності організації до реагування на різноманітні загрози. Ландшафт

кіберзагроз постійно розвивається, з'являються нові вектори атак та цілі, тому організації повинні адаптуватися та своєчасно модернізувати свої підходи до управління інцидентами. Важливо усвідомлювати, що ефективне управління інцидентами вимагає системного підходу та залучення відповідних ресурсів, включаючи організаційну культуру, навички персоналу, чіткі процеси та безперервне навчання.

Крім того, співпраця та обмін інформацією як всередині організації, так і між різними організаціями та галузями, є ключовим фактором для підвищення обізнаності про загрози та розповсюдження найкращих практик управління інцидентами. Участь у галузевих об'єднаннях, форумах та ініціативах з кібербезпеки може забезпечити цінні можливості для навчання та обміну досвідом.

Нарешті, слід пам'ятати, що управління інцидентами інформаційної безпеки – це динамічний та безперервний процес, який вимагає постійного вдосконалення та адаптації до нових викликів та змін у середовищі загроз. Організації, які впроваджують ефективні процеси управління інцидентами, інвестують у необхідні ресурси та беруть активну участь у галузевій співпраці, матимуть кращі шанси захистити свої цінні інформаційні активи та забезпечити безперервність своєї діяльності у мінливому світі кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ ISO/IEC 27035-1:2018 (ISO/IEC 27035-1:2016, IDT). Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80309.

2. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII.

3. ДСТУ ISO/IEC 27001:2015 - (ISO/IEC 27001:2013; Cor 1:2014, IDT) Методи захисту системи управління інформаційною безпекою. Вимоги. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910.

4. NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide. National Institute of Standards and Technology, 2012. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (дата звернення: 19.05.2024).

5. NIST Risk Management Framework | CSRC: Federal Information Security Modernization Act (FISMA) Background. URL: https://csrc.nist.gov/Projects/risk-management/fisma-background (дата звернення: 20.05.2024).

6. FIRST - Improving Security Together. URL: https://www.first.org/about/history (дата звернення: 20.05.2024)

7. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf

8. ДСТУ ISO/IEC 27035-2:2018 (ISO/IEC 27035-2:2016, IDT) Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80310.

9. SANS Institute. Incident Handler's Handbook. URL: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901 (дата звернення: 19.05.2024).

10. CERT/CC. CERT Incident Handling Process. URL: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508099 (дата звернення: 19.05.2024).

11. ITIL Incident Management Process. URL: https://www.axelos.com/best-practice-solutions/itil/what-is-itil/itil-processes/incident-management (дата звернення: 19.05.2024).

12. Бєлов О.В., Лєнков С.В., Корченко О.Г. Методологія формування стратегії управління інформаційною безпекою. Київ: Наукова думка, 2018. 312 с.

13. Петрик В.А., Кузнецова Н.В., Левченко О.Г. Управління інформаційною безпекою підприємства. Львів: Видавництво Львівської політехніки, 2020. 284 с.

14. Корченко О.Г., Ахметов Б.Б., Гнатюк С.О. Методи та засоби управління інцидентами інформаційної безпеки. Київ: ТОВ "НВП Інтерсервіс", 2020. 352 с.

15. Корченко О.Г. Методологічні основи управління інформаційною безпекою сучасних телекомунікаційних систем. Київ: ТОВ "НВП Інтерсервіс", 2017. 468 с.

16. Карпінський Н.П., Карпінська І.Ю. Управління інформаційними ризиками. Львів: Видавництво Львівської політехніки, 2021. 216 с.

17. Корченко О.Г., Гнатюк С.О., Козачок В.І. Методи та засоби протидії кіберінцидентам в інформаційно-телекомунікаційних системах. Київ: ТОВ "НВП Інтерсервіс", 2019. 416 с.

18. Бурячок В.Л., Толубко В.Б., Хохлачова Ю.Є., Іванов В.Г. Управління інформаційною безпекою в умовах гібридних загроз. Київ: ДУТ, 2020. 352 с.

19. Петрик В.А., Кузнецова Н.В., Левченко О.Г. Управління інформаційною безпекою в умовах Інтернету речей. Львів: Видавництво Львівської політехніки, 2022. 288 с.

20. Бурячок В.Л., Толубко В.Б., Хохлачова Ю.Є., Бєлов О.В. Управління ризиками інформаційної безпеки. Київ: ДУТ, 2021. 320 с.

21. Гладиш С. В., Кононович В. Г., Тардаскін М. Ф. Порівняльний аналіз стандартів ISO / IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2007. – № 15. – С. 31-39.

22. Кузнецов В.Ю., Хахановський В.Г., Козловський В.В. Управління інформаційною безпекою в умовах кібернетичного простору. Харків: ХНУРЕ, 2021. 312 с.

23. Бурячок В.Л., Толубко В.Б., Хохлачова Ю.Є., Остапов С.Е. Управління інформаційною безпекою в умовах кіберконфлікту. Київ: ДУТ, 2022. 296 с.

24. Шелест М.Є., Бурячок В.Л., Райко В.Ф. Основи управління інформаційною безпекою. Київ: ДУТ, 2022. 408 с.

25. Гладиш С. В. Інтелектуальна система керування інцидентами інформаційної безпеки телекомунікаційних мереж // Матеріали міжнародної науково-практичної конференції «Інформаційні технології та інформаційна безпека в науці, техніці та освіті ІНФОТЕХ 2007». – Севастополь: СевНТУ, 2007. – С. 53-57.

26. Гладиш С. В. Кононович В. Г. Реагування та обробка інцидентів інформаційної безпеки мультиагентною системою // Наукові праці Одеської національної академії зв'язку ім. О. С. Попова. – 2007.

27. Бурячок В.Л., Гнатюк С.О., Корченко О.Г. Управління інцидентами інформаційної безпеки в автоматизованих системах. Київ: ДУТ, 2019. 248 с.

28. Корченко О.Г., Бєлов О.В., Лєнков С.В. Методи та засоби забезпечення інформаційної безпеки в автоматизованих системах управління. Київ: Наукова думка, 2021. 384 с.

29. Корченко О.Г., Ахметов Б.Б., Гнатюк С.О. Методи та засоби управління інцидентами інформаційної безпеки в системах критичної інфраструктури. Київ: ТОВ "НВП Інтерсервіс", 2023. 408 с.

30. Петрик В.А., Кузнецова Н.В., Левченко О.Г. Управління інформаційною безпекою організації в умовах цифрової трансформації. Львів: Видавництво Львівської політехніки, 2022. 312 с.

31. Бурячок В.Л., Толубко В.Б., Хохлачова Ю.Є., Гнатюк С.О. Управління інцидентами інформаційної безпеки в корпоративних мережах. Київ: ДУТ, 2023. 280 с.

32. Петрик В.А., Кузнецова Н.В., Левченко О.Г. Управління інформаційною безпекою в умовах хмарних обчислень. Львів: Видавництво Львівської політехніки, 2021. 248 с.

33. Бурячок В.Л., Гнатюк С.О., Корченко О.Г. Управління інцидентами кібербезпеки в критичній інфраструктурі. Київ: ДУТ, 2022. 328 с.

34. Карпінський Н.П., Карпінська І.Ю. Управління інформаційною безпекою в умовах кіберзагроз. Львів: Видавництво Львівської політехніки, 2023. 272 с.

35. Корченко О.Г., Гнатюк С.О., Козачок В.І. Методи та засоби реагування на кіберінциденти в інформаційно-телекомунікаційних системах. Київ: ТОВ "НВП Інтерсервіс", 2021. 384 с.

36. Кузнецов В.Ю., Хахановський В.Г., Козловський В.В. Управління інформаційною безпекою в умовах кіберпростору. Харків: ХНУРЕ, 2022. 296 с.

37. Бурячок В.Л., Гнатюк С.О., Корченко О.Г. Управління інцидентами інформаційної безпеки в державному секторі. Київ: ДУТ, 2021. 304 с.

38. Карпінський Н.П., Карпінська І.Ю. Управління ризиками інформаційної безпеки в умовах цифрової трансформації. Львів: Видавництво Львівської політехніки, 2023. 240 с.

39. Корченко О.Г., Ахметов Б.Б., Гнатюк С.О. Методи та засоби реагування на кібератаки в критичній інфраструктурі. Київ: ТОВ "НВП Інтерсервіс", 2022. 376 с.

40. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. /[Корченко О.Г.,Гнатюк С.О., Казмірчук С.В. та ін.]. – Київ : Центр навч.-наук. та наук.-пр.виданьНАСБ України, 2014. –190 с. URL:

https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf

41. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с.

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

43. Донцов Є. А. Процеси управління інцидентами інформаційної безпеки в системах SIEM організації: матеріали Всеукр. наук.-практ. конф. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу . Київ : ДУІКТ, 28 лютого 2024. С. 17-19. URL: https://duikt.edu.ua/uploads/p_2661_62255520.pdf