МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ ЗАСОБИ ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ МЕРЕЖАХ”

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

_____ *Владислав ГАЛУШКО*

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42
Владислав ГАЛУШКО
Ім’я, ПРІЗВИЩЕ

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

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Галушко Владиславу Тарасовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Засоби виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах”,
керівник кваліфікаційної роботи ЯКИМЕНКО Юрій, к.в.н., доц.,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від 24.лютого 2025р. №56

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

3. Вихідні дані до кваліфікаційної роботи: *міжнародні стандарти, наукова та технічна література, методики управління ризиками, загрози та вразливості порушень ІБ*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати вплив процесів управління інцидентами інформаційної безпеки на функціонування корпоративних мереж.
4.2. Розглянути методичні підходи до виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах.
4.3. Дослідження і розробка рекомендацій по використанню засобів виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Проаналізувати вплив процесів управління інцидентами інформаційної безпеки на функціонування корпоративних мереж	08.04.2025	
4.	Розглянути методичні підходи до виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах	15.04.2025	
5.	Дослідити і розробити рекомендацій по використанню засобів виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах	22.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	
7.	Оформлення роботи.	6.05.2025	
8.	Оформлення презентації.	9.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

здобувач вищої освіти _____ Владислав ГАЛУШКО
(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 Галушко В.Т. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Засоби виявлення та класифікація інцидентів інформаційної безпеки в корпоративних мережах"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ,д.т.н., професор _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ГАЛУШКО Владислав у кваліфікаційній роботі проаналізував процеси управління ризиками інформаційної безпеки організації; використав методи аналізу, порівняння, класифікації, із системним підходом до аналізу засобів виявлення та класифікації інцидентів інформаційної безпеки; дослідив засоби виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах; розробив практичні рекомендації за темою дослідження.

ГАЛУШКО Владислав 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 ГАЛУШКО Владислава 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)*

"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Галушко Владислав допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ГАЛУШКО Владислава
на тему “Засоби виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах”

Актуальність. Сучасні організації зіштовхуються доволі часто з проблемами які так чи інакше є наслідками кіберінцидентів. Метою таких засобів є попередження та виявлення таких інцидентів та пророблення відповідних дій з усунення та отримання досвіду для майбутніх інцидентів.

Розробці засобів виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах приділяється все більше уваги, тому тема роботи, пов’язана з аналізом процесів управління ризиками інформаційної безпеки організації, є актуальною.

Позитивні сторони.

1. У роботі досліджено та проаналізовано впливу процесів управління інцидентами інформаційної безпеки на функціонування корпоративних мереж
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки.
3. Автор опрацював та дослідив значну джерельну базу: близько 25 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо впровадження та використання засобів виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах для протидії актуальним загрозам у корпоративному середовищу .

Недоліки.

Доцільно було б збільшити розмір шрифту тексту в елементах рисунків – для кращого сприймання.

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 ГАЛУШКО Владислав заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
к.т.н., доцент _____ *підпис* _____ Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена аналізу засобів виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах. Робота складається зі вступу, трьох розділів, що містять 9 рисунків і 6 таблиць, висновків і списку використаних джерел із 42 найменувань. Загальний обсяг роботи становить 71 аркуш, з яких 5 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є аналіз засобів виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах.

Об'єктом дослідження є засоби виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах.

Предмет дослідження є сучасні підходи та методи виявлення і класифікації інцидентів інформаційної безпеки в корпоративних мережах.

Методи дослідження. Для вирішення поставленого наукового завдання у роботі використано методи аналізу, порівняння, а також системний підхід до аналізу засобів виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах.

Як результат у роботі досліджено особливості інформаційної безпеки в корпоративних мережах, проаналізовано існуючі засоби та методи виявлення і класифікації інцидентів, а також визначено їх вплив на ефективність реагування на загрози інформаційної безпеки.

Галузь застосування. Розроблені рекомендації можуть бути використані при вдосконаленні засобів виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах та їх впровадження.

Ключові слова: ЗАСОБИ ВИЯВЛЕННЯ, ЗАСОБИ КВАЛІФІКАЦІЇ, ЗАГРОЗИ ТА ВРАЗЛИВОСТІ, ІНФОРМАЦІЙНА БЕЗПЕКА, ОЦІНКА РИЗИКІВ ІНЦИДЕНТІВ.

ABSTRACT

The qualification work is devoted to the analysis of the organization's information security risk management processes. The work consists of an introduction, three sections containing 9 drawings and 6 tables, conclusions and a list of used sources from 42 denominations. The total amount of work is 71 sheets from which 5 sheets contain a list of conventional abbreviations and a list of used sources.

The purpose of the study the analysis of tools for detecting and classifying information security incidents in corporate networks.

The object the study is tools for detecting and classifying information security incidents in corporate networks.

The subject of the study is modern approaches and methods for detecting and classifying information security incidents in corporate networks.

Research methods. To solve the scientific task, the work uses methods of analysis, comparison, as well as a systematic approach to the analysis of tools for detecting and classifying information security incidents in corporate networks..

As a result, the features of information security in corporate networks were investigated, existing tools and methods for detecting and classifying incidents were analyzed, and their impact on the effectiveness of responding to information security threats was determined.

Field of application. The developed recommendations can be used to improve the tools for detecting and classifying information security incidents in corporate networks and their implementation.

Keywords: DETECTION TOOLS, CLASSIFICATION TOOLS, THREATS AND VULNERABILITIES, INFORMATION SECURITY, INCIDENT RISK ASSESSMENT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

APT	Складна цілеспрямована загроза
IDS	Система виявлення вторгнень
IPS	Система запобігання вторгненням
TIP	Платформи кіберрозвідки загроз
DPI	Глибокий аналіз пакетів
ШІ	Штучний інтелект
SOAR	Оркестрація, автоматизація та реагування в сфері безпеки
IRT	Команда реагування на інциденти
NBAD	Виявлення аномалій у мережевій поведінці
MITM	Атака «людина посередині»
CIA	Конфіденційність, цілісність та доступність
NLP	Обробка природної мови
SIEM	Система керування інформацією та подіями безпеки

ВСТУП

Актуальність теми. Інформаційні технології відіграють важливу роль у функціонуванні будь-якої організації. Особливо це помітно в сучасних умовах цифрових технологій, коли корпоративні мережі є основою функціонування бізнесу, державних установ та інших організацій, зростає кількість загроз, пов'язаних з інцидентами інформаційної безпеки. Наявність великої кількості взаємопов'язаних систем, різноманіття мережевих пристроїв та складність інфраструктури створюють сприятливі умови для реалізації атак, що можуть призвести до порушення цілісності, конфіденційності та доступності даних. Необхідність ефективного управління інцидентами інформаційної безпеки зумовлюється високою динамікою розвитку кіберзагроз, зростаючою кількістю складних атак, а також потребою забезпечення безперервного функціонування корпоративних мереж. У зв'язку з цим, тема дослідження засобів виявлення та класифікації інцидентів інформаційної безпеки набуває особливої актуальності як з практичної, так і з наукової точки зору.

Метою роботи є аналіз засобів виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах.

Об'єктом дослідження є засоби виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах.

Предмет дослідження є сучасні підходи та методи виявлення і класифікації інцидентів інформаційної безпеки в корпоративних мережах. Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Проаналізувати вплив процесів управління інцидентами інформаційної безпеки на функціонування корпоративних мереж.
2. Розглянути методичні підходи до виявлення та класифікації інцидентів інформаційної безпеки.
3. Дослідити наявні засоби виявлення та класифікації інцидентів інформаційної безпеки й надати практичні рекомендації щодо їх впровадження у корпоративних мережах.

Методи дослідження. У роботі використано методи аналізу та синтезу наукової і технічної інформації, порівняння існуючих підходів, класифікацію типів інцидентів, експертне оцінювання засобів виявлення інцидентів, а також системний підхід до забезпечення кібербезпеки корпоративних мереж.

Як результат у роботі досліджено засоби виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах, проаналізовано вплив процесів управління інцидентами на функціонування інформаційної інфраструктури організацій, розглянуто методичні підходи до ідентифікації інцидентів та оцінено ефективність застосування відповідних інструментів. Розроблено рекомендації щодо практичного впровадження засобів виявлення та класифікації інцидентів з метою підвищення рівня захищеності корпоративних мереж.

Практичне значення одержаних результатів. Отримані в результаті дослідження результати можуть бути використані для вибору та впровадження ефективних засобів виявлення та класифікації інцидентів інформаційної безпеки у корпоративному середовищі. Це дозволить забезпечити підвищення рівня кіберзахищеності, зниження ризику порушення критичних бізнес-процесів і мінімізацію потенційних збитків, пов’язаних з інцидентами інформаційної безпеки.

Апробація результатів. Результати дослідження за темою “Засоби виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах” були апробовані на Всеукраїнській науково-практичній конференції “Інформаційна безпека в умовах цифровізації”, що відбулася __ червня 2025 року.

Розділ 1 АНАЛІЗ ВПЛИВУ ПРОЦЕСІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ФУНКЦІОНУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ

У цьому розділі розглядається вплив процесів управління інцидентами інформаційної безпеки на ефективність функціонування корпоративних мереж, зокрема, їхня роль у забезпеченні безперервності роботи, швидкому реагуванні на загрози та мінімізації наслідків порушень безпеки. Далі аналізуються сучасні підходи до організації реагування на інциденти, а також нормативні вимоги й практичні приклади впровадження систем реагування в корпоративному середовищі. Аналіз, проведений у межах цього розділу, покликаний продемонструвати важливість не лише технічних рішень, але й організаційної підготовки до інцидентів. Адже навіть наявність передових засобів виявлення не гарантує ефективного реагування у разі відсутності чітко визначеної структури, розподілу ролей та сценаріїв дій. Таким чином, розділ закладає теоретичну й концептуальну основу для подальшого розгляду методичних підходів до виявлення, класифікації та попередження інцидентів інформаційної безпеки в наступних розділах дослідження.

1.1. Аналіз вимог української нормативної бази в частині управління інцидентами інформаційної безпеки

Забезпечення належного управління інцидентами інформаційної безпеки є однією з ключових складових кіберзахисту корпоративних мереж. В Україні правове та нормативне регулювання у цій сфері базується на ряді законодавчих актів, підзаконних нормативів та галузевих стандартів, які визначають вимоги до суб’єктів кібербезпеки щодо виявлення, класифікації, фіксації та реагування на інциденти.

Ключовим документом, що регулює сферу кібербезпеки, є Закон України “Про основні засади забезпечення кібербезпеки України” від 5 жовтня 2017

року. У цьому законі вперше на рівні законодавства було введено поняття кіберінциденту, а також визначено перелік основних суб'єктів забезпечення кібербезпеки держави, серед яких: Національний координаційний центр кібербезпеки, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ), Національна поліція тощо. Стаття 9 цього закону зобов'язує власників або ж розпорядників критичної інфраструктури впроваджувати заходи для виявлення, запобігання та реагування на кіберінциденти, а також повідомляти уповноважені органи про факти порушення кібербезпеки.

"Власники або розпорядники об'єктів критичної інформаційної інфраструктури зобов'язані в порядку, визначеному Уповноваженим органом для функціонування національної системи обміну інформацією про кіберінциденти, кіберзагрози, кібератаки, повідомляти відповідний CSIRT про всі значні кіберінциденти."|

Додаткове нормативне підґрунтя забезпечується Законом України "Про захист інформації в інформаційно-телекомунікаційних системах", де визначаються загальні вимоги до захисту інформації та обов'язки власників інформаційних систем щодо створення комплексної системи захисту, яка має передбачати й функції фіксації та аналізу інцидентів. Українська нормативна база забезпечує формальні вимоги до управління інцидентами інформаційної безпеки, особливо в державному та критичному секторі. Водночас, залишається низка проблем: відсутність чітких вимог для приватного бізнесу, недостатня деталізація механізмів обміну інформацією про інциденти, обмежена кількість фахових методичних рекомендацій та фрагментарне впровадження сучасних технічних рішень SIEM, SOAR, автоматизація реагування). Зважаючи на викладене, можна стверджувати, що нормативна база України у сфері інформаційної безпеки створює формальні умови для організації процесів управління інцидентами. Проте її ефективність значною мірою залежить від рівня практичного впровадження в корпоративному середовищі. Для компаній, що не належать до сектору критичної інфраструктури, ці вимоги часто

залишаються рекомендаційними, що призводить до фрагментарного або декларативного підходу до управління інцидентами.

Окрему увагу варто приділити проблематиці розподілу відповідальності між суб'єктами, залученими до процесів забезпечення кібербезпеки. Як вказується в аналітичній записці Національного інституту стратегічних досліджень, чинна нормативно-правова база України не містить чітких положень щодо координації дій між органами державної влади, правоохоронними структурами та суб’єктами господарювання у разі виникнення інцидентів інформаційної безпеки. Відсутність усталеного механізму взаємодії між цими суб’єктами значно ускладнює ефективне реагування на кіберінциденти, особливо в умовах динамічного розвитку загроз. Зокрема, не унормовано питання оперативного обміну інформацією про інциденти між державними органами та приватними компаніями, що створює розриви в інформаційному ланцюгу та знижує ефективність заходів протидії. Крім того, відсутність централізованого органу, відповідального за моніторинг, класифікацію та координацію дій у випадку масштабних кібератак, ускладнює формування єдиної політики реагування в національному масштабі. Це, у свою чергу, позначається і на діяльності корпоративних мереж, які залишаються вразливими через нерозвинену систему попередження інцидентів на рівні держави.

Недостатня деталізація механізмів взаємодії з державними органами, нечіткість у процедурі реєстрації інцидентів, а також брак стандартизованих методик ведуть до того, що процеси виявлення та реагування реалізуються з великим запізненням або взагалі відсутні. Це безпосередньо впливає на стійкість корпоративних мереж до зовнішніх та внутрішніх загроз, збільшує час виявлення вторгнень, а в деяких випадках – призводить до втрати критичної інформації або зупинки бізнес-процесів.

1.2. Аналіз досліджень з виявлення проблем в управлінні інцидентами інформаційної безпеки при функціонуванні корпоративних мереж

Проблематика ефективного управління інцидентами інформаційної безпеки активно досліджується як у вітчизняному, так і в міжнародному науково-практичному дискурсі. В умовах динамічного розвитку загроз корпоративні мережі стикаються з комплексом викликів, які ускладнюють процеси виявлення, класифікації та реагування на інциденти. Згідно з даними міжнародного звіту IBM X-Force Threat Intelligence (2023), середній час перебування зловмисника в мережі до моменту його виявлення становить понад 200 днів, що свідчить про серйозні дефіцити у системах раннього оповіщення та внутрішнього моніторингу.

Значну частину виявлених проблем складають технічні чинники. До таких належать: фрагментарність інструментів безпеки, відсутність повноцінно інтегрованих SIEM-рішень, а також обмежене застосування сучасних засобів аналізу поведінкових аномалій. У корпоративному середовищі досі переважають рішення, орієнтовані на сигнатурне виявлення атак, що не дає змоги ідентифікувати нові або складно-структуровані типи інцидентів тощо. Організаційні недоліки відіграють не менш критичну роль. У багатьох підприємствах відсутні затверджені та протестовані плани реагування на інциденти, а роль і повноваження персоналу з інформаційної безпеки часто залишаються нечітко визначеними. Внутрішні інструкції або не актуалізуються, або не охоплюють повного спектра можливих сценаріїв інцидентів. Така ситуація призводить до неузгоджених дій між підрозділами, затримок у прийнятті рішень та хаотичного реагування на інциденти без урахування їх критичності.

Проблемним виявляється і кадровий аспект. За результатами дослідження ISACA (2023), понад 60% IT-керівників вказують на брак кваліфікованих фахівців з безпеки в межах своїх організацій. Ситуація ускладнюється ще й

тим, що існуючі навчальні програми з кібербезпеки часто не встигають за динамікою розвитку загрозового ландшафту. Тому навіть наявність сертифікацій не завжди гарантує належний рівень практичної готовності фахівця до реагування на сучасні інциденти. Це підкреслює потребу в постійному професійному розвитку персоналу через участь у тренінгах, хакатонах та симуляційних навчаннях. Низький рівень технічної компетенції у поєднанні з відсутністю сценарного моделювання інцидентів зменшує шанси на ефективне реагування навіть за наявності відповідного технічного забезпечення. Ця тенденція простежується також в Україні, де більшість підприємств малого і середнього бізнесу не мають штатних аналітиків SOC або інженерів з реагування на інциденти, що підвищує залежність від сторонніх сервісних провайдерів.

Нині розвиток технологій машинного навчання та штучного інтелекту набирає стрімкого розвитку, однак більшість організацій і далі покладаються на ручне сортування інцидентів за ступенем критичності. Це уповільнює процеси ескалації, підвищує ризик помилкової пріоритезації та створює загрозу ігнорування критичних подій на фоні великої кількості малозначущих сповіщень. Накопичений масив досліджень дозволяє виокремити типові проблеми, що істотно знижують ефективність реагування на інциденти та ускладнюють їх класифікацію в умовах реального часу.

Одна з найпоширеніших проблем – затримка у виявленні порушень безпеки. Так, за даними галузевих аналітичних звітів IBM X-Force Threat Intelligence Report (2023), середній час, що минає між фактичним початком інциденту та його виявленням перевищує 200 діб. У корпоративному контексті це означає тривалий період невиявленого доступу до критичних систем, що створює передумови для глибшої компрометації та створенню відповідних загроз.

Суттєвим ускладненням є також фрагментарність підходів до фіксації та обробки подій безпеки. У більшості організацій відсутні централізовані системи кореляції подій SIEM, або такі системи не інтегровані з іншими

засобами мережевого захисту. Як наслідок, спостерігається розрив між вхідними потоками даних про події та можливістю оперативно їх аналізувати. Це призводить до зниження інформованості фахівців з інформаційної безпеки щодо контексту інцидентів.

Відповідно до стандарту ISO/IEC 27035, процес реагування на інциденти включає п’ять основних фаз: підготовка, виявлення і повідомлення, оцінка та прийняття рішень, реагування, а також навчання на основі результатів. Проте у практичному застосуванні ці фази часто стикаються з низкою проблем, які негативно впливають на ефективність виявлення і мінімізацію наслідків кіберінцидентів.

Однією з найбільш поширених проблем є затримка у виявленні інциденту. Незважаючи на те, що стандарт визначає потребу у своєчасному виявленні, на практиці інциденти можуть залишатися непоміченими протягом тривалого часу, що пов'язано з недостатньою інтеграцією систем моніторингу, низькою обізнаністю персоналу або неефективним застосуванням автоматизованих засобів аналітики. Це створює значні ризики для безперервності бізнес-процесів і сприяє зростанню операційних збитків.

Дослідження у сфері інформаційної безпеки свідчать про недостатнє документування та стандартизацію процедур реагування, що ускладнює повторне використання знань і послаблює здатність організації до адаптивного навчання. За відсутності чітко визначеної ролі та відповідальності серед членів команди реагування, можливе дублювання дій або, навпаки, пропуск критичних етапів у ланцюжку реагування. Саме тому стандарт ISO/IEC 27035 наголошує на необхідності формування команд реагування, які діють відповідно до наперед узгоджених планів.

Варто також підкреслити проблему низької міжсистемної сумісності засобів виявлення, яка перешкоджає оперативному обміну інформацією між різними компонентами інфраструктури. З огляду на це, стандарт рекомендує впровадження централізованих систем логування і використання систем

управління інцидентами SIEM, що дозволяють акумулювати, аналізувати та корелювати події з різних джерел в режимі реального часу.

Дослідники також звертають увагу на проблеми організаційного характеру: невизначеність процедур реагування, дублювання відповідальності між підрозділами IT та інформаційної безпеки, а також відсутність затверджених планів дій у разі інцидентів.

Низька кваліфікація персоналу залишається додатковим обтяжуючим чинником. Відсутність фахівців з досвідом роботи із системами виявлення атак, обмежене розуміння методів аналізу поведінки зловмисників, а також низька обізнаність працівників щодо процедур повідомлення про інциденти створюють ризик запізнілого реагування навіть при наявності технічних засобів моніторингу.

Також спостерігається недостатній рівень автоматизації процесів класифікації та пріоритезації інцидентів. У більшості випадків рішення щодо важливості інциденту приймаються вручну, що суттєво знижує швидкість реагування та ускладнює масштабування процесів безпеки в умовах зростання кількості подій.

Висновок до розділу 1

На основі здійсненого аналізу можна дійти висновку, що процеси управління інцидентами інформаційної безпеки є критично важливими для забезпечення стабільного та безпечного функціонування корпоративних мереж. Розгляд нормативної бази, типів загроз, а також ключових проблем, пов’язаних з організацією реагування, дає підстави стверджувати, що ефективне управління інцидентами потребує цілісного підходу, в якому поєднуються технічні, процедурні, кадрові та нормативні елементи.

Однією з найпомітніших проблем виявляється людський чинник, зокрема недостатня кількість спеціалістів, низький рівень обізнаності співробітників щодо основ інформаційної безпеки та відсутність практики регулярних навчань

чи моделювань інцидентів. Також актуальним залишається питання слабкої інтеграції засобів захисту, що ускладнює комплексну обробку подій та координацію дій у разі кризи.

Загалом можна стверджувати, що ефективне реагування на інциденти можливе лише за умови синергії організаційних заходів, сучасних технологічних рішень і системного підходу до оцінки ризиків. Отримані висновки формують підґрунтя для подальшого дослідження методичних підходів до виявлення та класифікації інцидентів, що буде розглянуто у наступному розділі.

Розділ 2 РОЗГЛЯД МЕТОДИЧНИХ ПІДХОДІВ ДО ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ МЕРЕЖАХ

У цьому розділі проводиться аналіз методичних підходів до виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах, а також оцінюється їх ефективність. Розглядаються принципи побудови систем виявлення інцидентів, класифікаційні ознаки загроз, особливості застосування сучасних технологій і засобів, що забезпечують своєчасне реагування на порушення безпеки. Особливу увагу приділено поведінковим моделям, які ґрунтуються на аналізі дій користувачів і пристроїв, а також технологіям обробки великих обсягів даних у рамках систем типу SIEM, UEBA, SOAR. Їхнє застосування дозволяє відійти від традиційних сигнатурних методів, які стають дедалі менш ефективними в умовах постійного оновлення способів обходу захисту. Таким чином, розділ має на меті створити цілісне уявлення про сучасні інструменти й концептуальні підходи до боротьби з інцидентами в корпоративному кіберпросторі.

2.1. Аналіз загроз інформаційної безпеки для корпоративних мереж

Серед найпоширеніших типів загроз виділяють зловмисне програмне забезпечення (malware), шифрувальники (ransomware), цільові фішингові кампанії (spear phishing), атаки типу "людина посередині" (MitM), відмови у обслуговуванні (DDoS), а також експлуатацію вразливостей у доступному програмному забезпеченні. Окрему категорію становлять інсайдерські загрози, які можуть мати навмисний або ненавмисний характер і здатні призвести до витоку конфіденційної інформації чи порушення цілісності систем. Ненавмисні інсайдерські інциденти часто спричинені помилками користувачів, які не мають злого наміру, однак через недостатню обізнаність або ігнорування політик безпеки відкривають вектори для атак. Типовими прикладами є використання

слабких паролів, неконтрольоване завантаження файлів або натискання на фішингові посилання. Профілактика таких інцидентів передбачає не лише контроль доступу, а й систематичну просвітницьку роботу з персоналом. Для систематизації типових ризиків доцільно навести узагальнений перелік основних загроз, які найчастіше реалізуються в корпоративних мережах (див. табл. 2.1.).

Таблиця 2.1.

Перелік основних загроз інформаційної безпеки для корпоративних мереж

Категорія загроз	**Приклади**
Malware	Віруси, трояни, руткіти, програми-шпигуни
Ransomware	WannaCry, LockBit, Ryuk
Phishing	E-mail, SMS, spear phishing
DDoS	UDP flood, HTTP flood
Внутрішні загрози	Навмисні та ненавмисні дії працівників
Вразливості ПЗ	Zero-day, незакриті CVE
Соціальна інженерія	Pretexting, baiting

Традиційні системи виявлення загроз, зокрема сигнатурні антивірусні платформи та класичні IDS-рішення, базуються на принципі відповідності заздалегідь відомим шаблонам шкідливої активності. Однак у випадках складних, багатофазних атак цей підхід часто виявляється неефективним, оскільки зловмисники активно використовують техніки обфускації, поліморфізму, а також змінюють шаблони поведінки. Як результат, сигнатурні рішення фіксують лише симптом, а не суть проблеми, що знижує ефективність протидії загрозам у реальному часі. Це спонукає організації до впровадження більш гнучких, поведінкових підходів, таких як UEBA або SIEM з елементами

машинного навчання. Бо саме в умовах швидкої еволюції загроз, зокрема з використанням zero-day векторів та обфускації, підхід, орієнтований на сигнатури, дедалі частіше виявляється недостатнім. З цієї причини актуальним стає поведінковий аналіз користувачів – UEBA, що орієнтується не на фіксацію статичних ознак загрози, а на виявлення відхилень від нормальної поведінки об’єктів.

UEBA-системи, такі як реалізовані у продуктах IBM Security, дозволяють сформувати динамічну модель типової активності користувачів, пристроїв або сервісів на основі історичних даних. Подальше спостереження за аномаліями, які виходять за межі встановлених моделей (наприклад, спроба доступу до нетипових ресурсів у нестандартний час або перенесення великого обсягу даних за межі організації), створює умови для раннього попередження про інцидент ще до його ескалації.

2.1.1. Виявлення підозрілої поведінки користувачів

Виявлення аномальної поведінки користувачів у корпоративних мережах здійснюється за допомогою методів поведінкового аналізу UEBA, які базуються на побудові профілів типової активності. Цей процес є багаторівневим (див. рис. 2.1.). Відхилення від виведених моделей фіксуються як ознаки потенційного інциденту безпеки. Типовими показниками такої активності є: перенесення великих обсягів інформації за короткий проміжок часу; повторні спроби входу з нових геолокацій; нетипові взаємодії, які зазвичай не зустрічаються у сфері діяльності користувача; тощо. UEBA-системи функціонують шляхом збору та кореляції подій з журналів аутентифікації, активності у файлових системах, спроб ескалації привілеїв та нестандартних з’єднань.

Рис. 2.1. Загальний принцип роботи UEBA-системи

Для формалізації моделей поведінки застосовуються методи машинного навчання: кластеризація (k-means), багатовимірне скорочення розмірності (PCA), ймовірнісні моделі (наприклад, HMM), а також дерева ізоляції (Isolation Forest) для виявлення нетипових випадків. На відміну від сигнатурних підходів, ці методи дозволяють враховувати контекст поведінки конкретного користувача: часові шаблони, роль у системі, типові обсяги трафіку або доступу.

Функціонально UEBA складається з трьох рівнів: модуль збору та нормалізації даних, аналітичне ядро з алгоритмами поведінкового аналізу та інтерфейс для розслідування інцидентів. У деяких реалізаціях система взаємодіє з SIEM-платформами для автоматизованої ескалації або блокування активності. Впровадження таких систем потребує наявності якісного логування, чітко визначених ролей у системі доступу, а також розмежування звичайних та критичних дій. Крім того, важливо забезпечити регулярне оновлення

поведінкових профілів та обробку хибнопозитивних спрацювань, що виникають внаслідок зміни режиму роботи, службових обов'язків або тимчасових розширень доступу.

Після впровадження систем UEBA, виникає низка технічних та організаційних викликів, які потребують ретельного опрацювання для забезпечення ефективного виявлення підозрілої поведінки користувачів. До таких викликів відносяться: управління хибнопозитивними спрацюваннями, якість та повнота даних, адаптація до змін у поведінці користувачів і забезпечення конфіденційності та відповідності нормативним вимогам

Управління хибнопозитивними спрацюваннями є однією з основних проблем при впровадженні UEBA є велика кількість хибнопозитивних спрацювань, коли нормальна поведінка користувача помилково ідентифікується як аномальна. Це може призвести до перевантаження команд безпеки та зниження ефективності реагування на реальні загрози. Для мінімізації таких випадків рекомендується використання багаторівневого аналізу, яке включає застосування алгоритмів машинного навчання, що враховують контекст поведінки користувача і дозволяє зменшити кількість хибнопозитивних спрацювань. Наприклад, система може ігнорувати одиничні аномалії і реагувати на сукупність підозрілих дій . Встановлення і налаштування відповідних порогових значень для виявлення аномалій допомагає уникнути надмірної чутливості системи до незначних відхилень у поведінці користувачів .

Якість та повнота даних використовуються для аналізу ефективності UEBA. Недостатня або нерелевантна інформація може призвести до неправильних висновків та зниження точності виявлення загроз. Рекомендується:

• Визначення релевантних джерел даних: Ідентифікація та інтеграція джерел, які надають найбільш цінну інформацію для аналізу поведінки користувачів, таких як журнали доступу, дії в системах та мережевий трафік.

• Забезпечення цілісності даних: Регулярна перевірка та оновлення даних, що використовуються для навчання моделей, допомагає підтримувати актуальність та точність аналізу.

Адаптація до змін у поведінці користувачів в робочих процесах, їх ролях або організаційних структурах можуть впливати на поведінкові шаблони, що використовуються UEBA для виявлення аномалій. Для адаптації до таких змін рекомендується:

• Регулярне оновлення моделей поведінки: Періодичне перенавчання моделей з урахуванням нових даних дозволяє системі адаптуватися до змін у поведінці користувачів .

• Використання контекстної інформації: Інтеграція додаткових даних, таких як інформація про відпустки, зміни в робочому графіку або нові проекти, допомагає точніше інтерпретувати поведінкові зміни.

Забезпечення конфіденційності та відповідності нормативним вимогам є важливим під час збирання і аналізу поведінкових даних користувачів. Для вирішення цих питань рекомендується:

• Анонімізація даних: застосування методів анонімізації дозволяє зберігати конфіденційність користувачів при аналізі їх поведінки.

• Відповідність нормативним стандартам: забезпечення відповідності політик обробки даних вимогам таких нормативних актів, як GDPR, допомагає уникнути юридичних ризиків .

Успішне впровадження та експлуатація систем UEBA вимагає комплексного підходу, що включає технічні, організаційні та етичні аспекти. Забезпечення якості даних, адаптація до змін у поведінці користувачів, управління хибнопозитивними спрацюваннями та дотримання нормативних вимог є ключовими факторами для ефективного виявлення підозрілої поведінки в корпоративних мережах.

2.1.2. Аналіз аномалій у мережевому трафіку

Основна мета такого аналізу – виявлення нетипових, потенційно шкідливих дій, які не можуть бути ідентифіковані сигнатурними методами, зокрема у випадках використання нових або модифікованих технік атак. Для реалізації систем виявлення аномалій у трафіку використовуються два основні підходи, як на табл. 2.2.

Таблиця 2.2.

Основні підходи виявлення аномалій у трафіку

Підходи до реалізації систем виявлення аномалій у трафіку	
Перший підхід	**Другий підхід**
Передбачає формування набору граничних параметрів та фіксацію їх перевищення. Наприклад, допустимі обсяги вхідного/ вихідного трафіку, кількість з'єднань за одиницю часу, тощо.	Ґрунтується на побудові моделей "нормального" трафіку для визначення відхилень, які не вкладаються у визначені закономірності.

Є низка ключових ознак, що можуть вказувати на наявність аномалій у трафіку (див. рис. 2.2.).

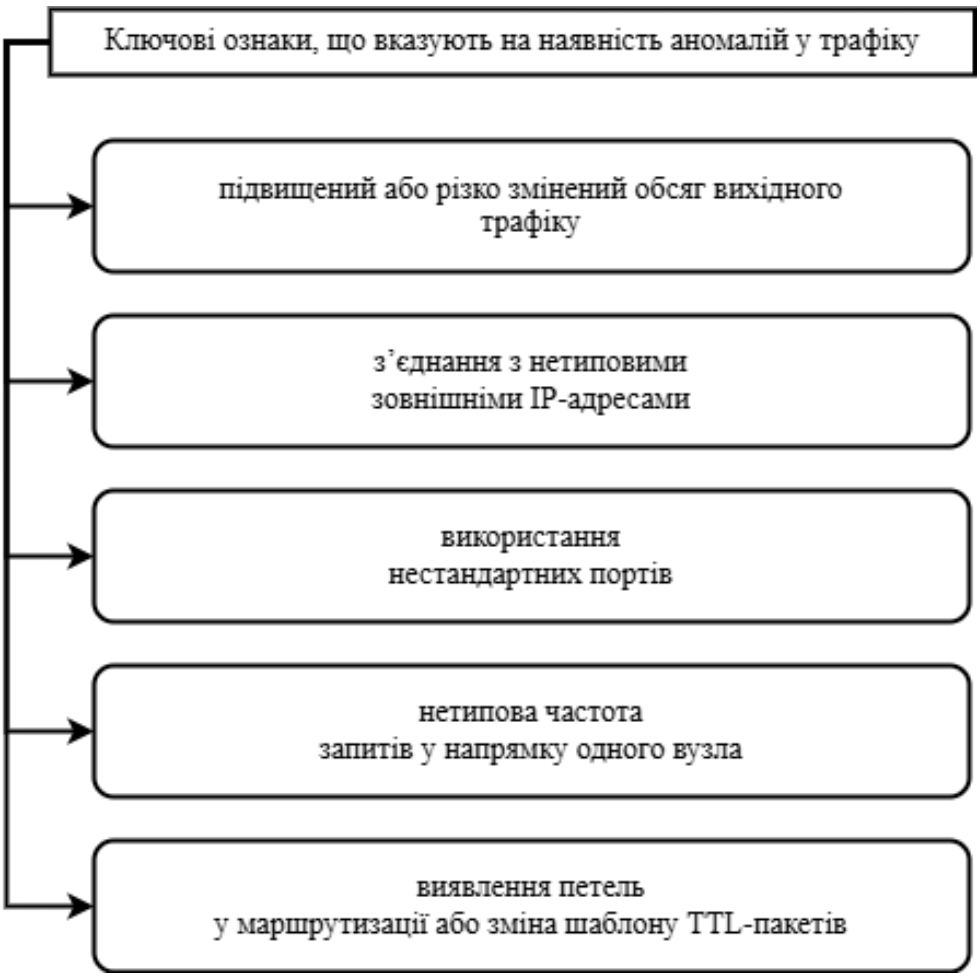

Рис.2.2. Ключові ознаки витоку інформації

Щоб краще ідентифікувати потенційні загрози, варто виокремити найтиповіші ознаки аномального трафіку, які найчастіше супроводжують інциденти (див. рис. 2.3).

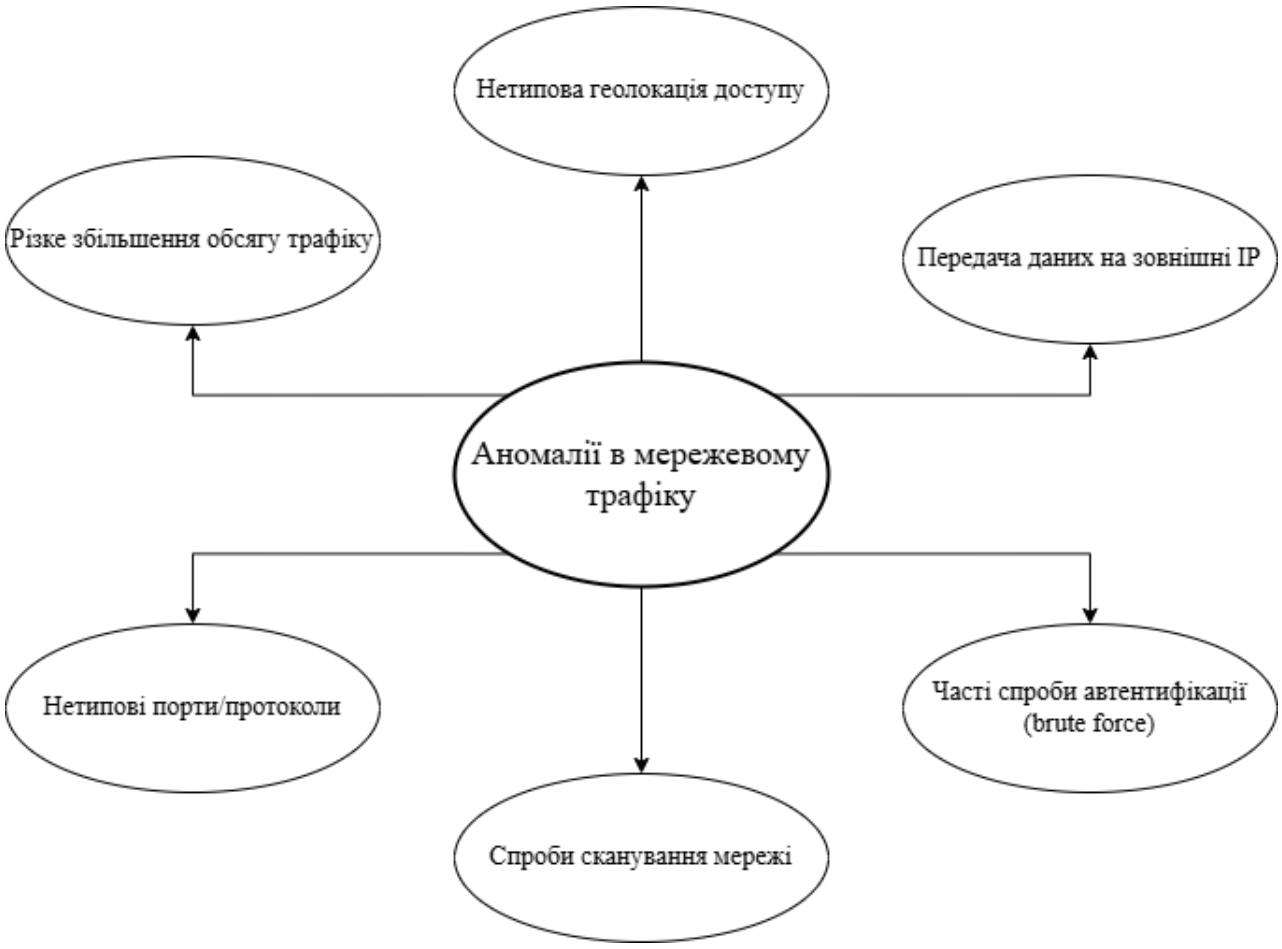

Рис. 2.3. Перелік аномалій у мережевому трафіку

Збір даних для аналізу трафіку здійснюється зазвичай з використанням протоколів NetFlow, sFlow, IPFIX, а також за допомогою мережевих сенсорів (наприклад, на базі Zeek. Дані обробляються у реальному часі або з затримкою в об'єднаному сховищі, інтегрованому з SIEM-рішенням або окремим модулем NBAD.

У рамках побудови моделі "нормального" мережевого профілю часто застосовуються методи кластеризації (наприклад, DBSCAN, k-means), зниження розмірності, а також байєсівські мережі для ідентифікації нетипових векторів трафіку. Зокрема, ізоляційні дерева (Isolation Forest) дозволяють ефективно виявляти рідкісні або унікальні зразки аномалій, особливо у великих потоках даних.

Однією з проблем, які спостерігаються при впровадженні аномалійного аналізу трафіку, є велика кількість «шуму», що виникає через природню, але

нестандартну поведінку користувачів або систем (наприклад, резервне копіювання в позаробочий час, хмарні обміни файлами, інтенсивне використання VPN). Для зменшення хибнопозитивних спрацьовувань є низка методів (див. табл. 2.3.).

Таблиця 2.3.

Рекомендації для зменшення хибно позитивних спрацьовувань

Методи зменшення хибнопозитивних спрацьовувань
впроваджувати **чорні та білі списки адрес та сервісів**
використовувати **інтеграцію з індикаторами компрометації (IoC)** та Threat Intelligence платформами
здійснювати попередню **сегментацію трафіку за ролями** та рівнями довіри

Важливо передбачити адаптивне перенавчання моделей та періодичне оновлення профілів нормального трафіку, оскільки зі зміною політик доступу або впровадженням нових сервісів зростає ризик неправильної інтерпретації подій.

2.2. Основні способи класифікації атак і загроз інформаційної безпеки в мережах

Ефективність системи захисту значною мірою залежить від точності і системності ідентифікації ворожих впливів, тому класифікація не є лише теоретичною процедурою, а й основою для побудови архітектури захисту, формування правил моніторингу та автоматизації реагування на інциденти.

Види класифікацій можуть суттєво відрізнятися залежно від мети: від технічного аналізу трафіку до стратегічної оцінки загрозових акторів.

Базові класифікації часто поділяють атаки за рівнем взаємодії з системою, за місцем реалізації або за походженням – внутрішні і зовнішні. Поширеним є також поділ за порушеним принципом моделі CIA, що дозволяє точно визначити, чи має атака на меті розкриття, зміну чи блокування даних і сервісів. Класифікація атак виконується за кількома критеріями, що відображає різні аспекти загроз. Узагальнений перелік основних класифікацій та деякі приклади подано на рис. 2.4.

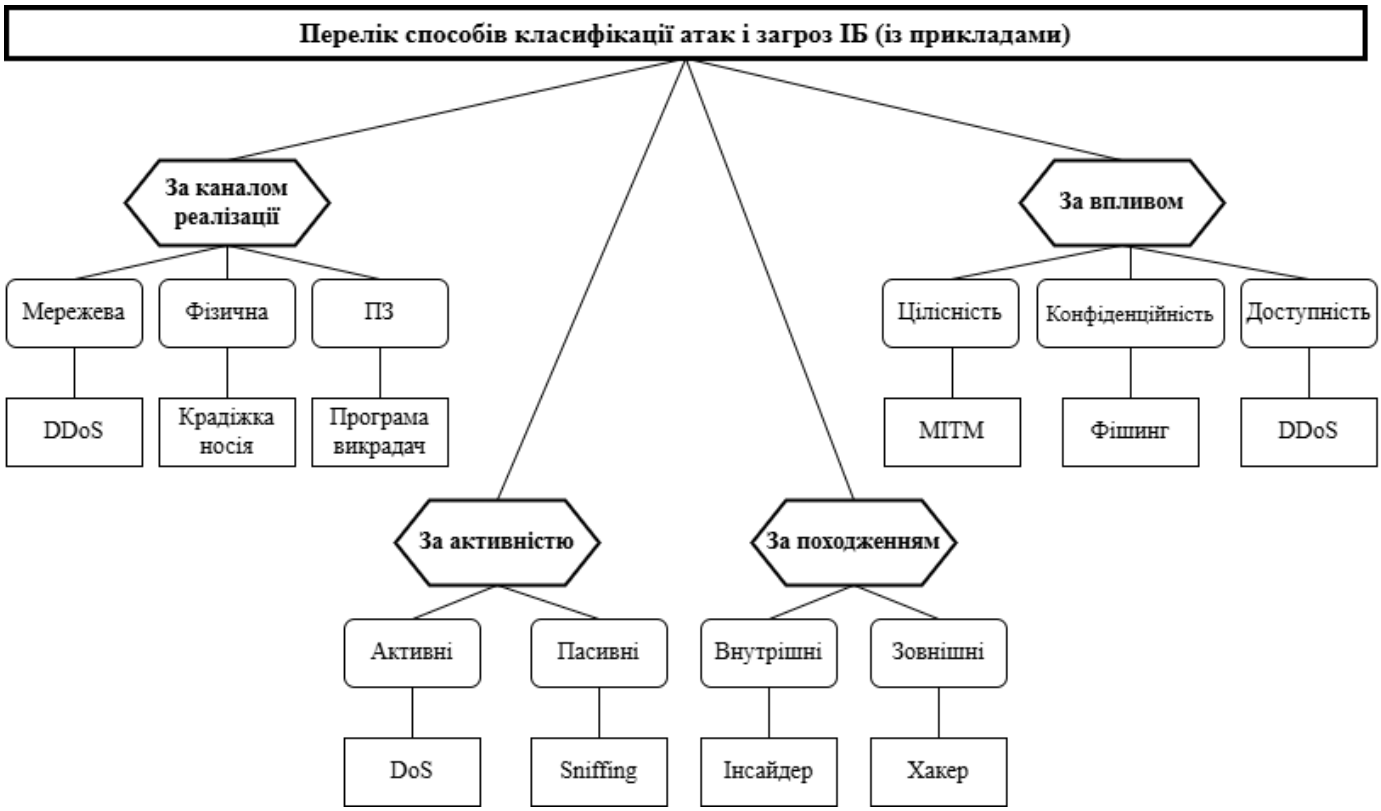

Рис. 2.4. Узагальнений перелік способів класифікації атак і загроз ІБ

2.2.1. Розподіл загроз за джерелом і типом атак

У сучасній науковій літературі з питань інформаційної безпеки класифікація загроз та атак за джерелом їх походження вважається одним із фундаментальних підходів до структурування знань про кіберзагрози. Аналіз

загроз за джерелом походження дозволяє не лише систематизувати існуючі типи атак, але й розробляти більш ефективні механізми захисту, спрямовані на конкретні категорії джерел загроз. Систематизація та структурування загроз за цим принципом є важливим елементом загальної системи управління інцидентами інформаційної безпеки.

Відповідно до досліджень Бурячка В.Л. та Толюпи С.В., джерела загроз інформаційній безпеці корпоративних мереж поділяються на три основні категорії, як показано в табл. 2.4.

Таблиця 2.4.

Види джерел загроз ІБ та їх приклади

Види джерел загроз інформаційній безпеці	
Антропогенні (людські)	• Насанкціонований доступ працівника • Фішинг • Нехтування правилами техніки безпеки
Техногенні (технічні)	• Відмова серверного обладнання • Збій у системі електропостачання • Помилки в програмному забезпеченні • Несправність систем резервного копіювання • Вразливості в мережевому обладнанні
Стихійні (природні)	• Повінь/Пожежа/Землетрус • Гроза (ураження блискавкою) • Екстремальні температури

При цьому антропогенні джерела загроз у контексті корпоративних мереж є найбільш різноманітними та становлять найсуттєвішу загрозу. За даними аналітичного звіту компанії “Verizon” за 2023 рік, понад 82% інцидентів інформаційної безпеки мають саме антропогенне походження.

Класифікація антропогенних джерел загроз передбачає їх поділ на зовнішні та внутрішні. До зовнішніх джерел загроз належать хакери, кіберзлочинці, конкуренти, терористи, іноземні розвідувальні служби, а також інші зловмисники, які не мають безпосереднього доступу до внутрішньої

інфраструктури організації. За дослідженнями Національного інституту стандартів і технологій США (NIST), зовнішні загрози характеризуються високим рівнем технічної складності та використанням передових технологій проникнення в системи. Зокрема, найпоширенішими типами атак із зовнішніх джерел є фішинг, використання шкідливого програмного забезпечення, DDoS-атаки, експлуатація вразливостей нульового дня та атаки типу "людина посередині".

Внутрішні джерела загроз включають штатних та колишніх співробітників організації, підрядників, партнерів та інших осіб, які мають легітимний доступ до інформаційних систем підприємства. Відповідно до досліджень Інституту інженерів електротехніки та електроніки (IEEE), інциденти, спричинені внутрішніми джерелами, часто мають більш руйнівні наслідки через високий рівень доступу інсайдерів до критичних систем та даних. При цьому важливо зазначити, що не всі інциденти, спричинені внутрішніми джерелами, є результатом зловмисних дій – значна частина таких інцидентів виникає через необережність, недостатню компетентність або нехтування правилами інформаційної безпеки.

Техногенні джерела загроз пов'язані з технічними помилками, збоями та відмовами апаратного і програмного забезпечення. До цієї категорії належать відмови обладнання, помилки в програмному коді, збої в роботі систем електроживлення, проблеми з мережевим обладнанням тощо.

Стихійні джерела загроз включають різноманітні природні явища, такі як пожежі, повені, землетруси, урагани та інші стихійні лиха, які можуть призвести до пошкодження інформаційної інфраструктури та порушення нормального функціонування корпоративних мереж. Хоча такі загрози становлять лише близько 5% від загальної кількості інцидентів, їх наслідки можуть бути катастрофічними через потенційне фізичне знищення інформаційних активів.

Класифікація загроз за типом атак є не менш важливим аспектом структурування знань про кіберзагрози. У науковій літературі виділяють різні

підходи до такої класифікації, однак найбільш поширеним є поділ атак на пасивні та активні. Пасивні атаки передбачають збір інформації без безпосереднього втручання в роботу інформаційних систем. До таких атак належать прослуховування мережевого трафіку, аналіз метаданих, моніторинг електромагнітного випромінювання тощо. Основною особливістю пасивних атак є складність їх виявлення, оскільки вони не призводять до безпосередніх змін у роботі систем.

Активні атаки, на відміну від пасивних, передбачають безпосереднє втручання в роботу інформаційних систем з метою порушення їх нормального функціонування, отримання несанкціонованого доступу до даних або компрометації системи безпеки. До активних атак належать атаки типу "відмова в обслуговуванні" (DoS та DDoS), впровадження шкідливого програмного забезпечення, атаки на веб-додатки, експлуатація вразливостей у програмному забезпеченні тощо.

З розвитком технологій з'являються нові, більш складні типи атак, які важко віднести до однієї конкретної категорії. Такі атаки часто називають гібридними або комплексними, оскільки вони поєднують елементи різних типів атак для досягнення максимальної ефективності. Наприклад, сучасні цільові атаки часто використовують комбінацію соціальної інженерії, експлуатації вразливостей у програмному забезпеченні та впровадження шкідливого коду.

Узагальнюючи різні підходи до класифікації загроз за джерелом і типом атак, можна запропонувати інтегровану таксономію загроз інформаційній безпеці корпоративних мереж, яка враховує як джерело загрози, так і тип атаки. Така таксономія дозволяє більш точно описувати та класифікувати інциденти інформаційної безпеки, що, у свою чергу, сприяє розробці більш ефективних стратегій захисту.

2.2.2. Поділ атак за механізмом впливу

Класифікація кібератак за механізмом впливу є важливим методологічним підходом, який дозволяє детально аналізувати способи здійснення атак та розробляти ефективні контрзаходи. У науковій літературі з інформаційної безпеки існує декілька підходів до такої класифікації, проте найбільш структурованим вважається поділ атак за механізмом впливу відповідно до моделі CIA – конфіденційність, цілісність, доступність. З метою наочності нижче подано узагальнену таблицю (див. табл. 2.5.), що ілюструє класифікацію атак за принципом моделі CIA.

Таблиця 2.5.

Способи класифікації атак за критеріями CIA

Критерій	**Типові атаки**	**Приклади**
Конфіденційність	Прослуховування, фішинг	Перехоплення логінів
Цілісність	Модифікація даних	Впровадження шкідливого коду
Доступність	• DDoS • Блокування сервісів	Масовані атаки на веб-ресурси

Атаки, спрямовані на порушення конфіденційності інформації, мають на меті несанкціонований доступ до конфіденційних даних. До таких атак належать різноманітні техніки несанкціонованого доступу, включаючи підбір паролів, перехоплення мережевого трафіку, соціальну інженерію, фішинг, використання бекдорів та троянських програм.

Особливу категорію атак на конфіденційність становлять криптографічні атаки, спрямовані на подолання механізмів шифрування. До них належать

атаки методом повного перебору (brute force), криптоаналітичні атаки, атаки за побічними каналами (side-channel attacks) тощо. З розвитком квантових обчислень проблема криптографічних атак набуває особливої актуальності, оскільки існуючі алгоритми шифрування, зокрема RSA та ECC, потенційно вразливі до атак з використанням квантових комп'ютерів.

Атаки, спрямовані на порушення цілісності даних, передбачають несанкціоновану модифікацію інформації. До таких атак належать модифікація мережевого трафіку, підміна веб-сторінок, ін'єкції коду (SQL-ін'єкції, XSS-атаки), атаки MITM. Відповідно до статистичних даних, наведених у звіті компанії “IBM” за 2023 рік, атаки на цілісність даних становлять приблизно 30% усіх зафіксованих інцидентів.

Атаки типу MITM заслуговують на окрему увагу, оскільки вони дозволяють зловмиснику не лише порушувати конфіденційність інформації через перехоплення даних, але й модифікувати їх у процесі передачі. Такі атаки часто реалізуються через компрометацію маршрутизаторів, підміну DNS-записів або через спеціально створені точки доступу Wi-Fi. Для захисту від атак типу MITM використовуються криптографічні протоколи з функціями автентифікації, такі як TLS/SSL, а також механізми перевірки цілісності даних, наприклад, цифрові підписи.

Атаки, спрямовані на порушення доступності інформації та сервісів, ставлять за мету обмеження або повне блокування доступу легітимних користувачів до інформаційних ресурсів. Найбільш поширеним типом таких атак є атаки типу DoS та їх більш складний варіант — розподілені атаки типу DDoS. Під час DDoS-атак використовуються розподілені мережі заражених комп'ютерів (ботнети) для генерації значного обсягу трафіку, спрямованого на цільову систему, що призводить до перевантаження її ресурсів та нездатності обслуговувати запити законних користувачів.

Відповідно до досліджень, проведених компанією “Cloudflare”, інтенсивність та масштаб DDoS-атак щороку зростають. У 2023 році було зафіксовано DDoS-атаки з піковою пропускною здатністю понад 3 Тбіт/с, що

значно перевищує можливості більшості організацій щодо фільтрації та обробки такого обсягу трафіку. Для захисту від DDoS-атак використовуються різноманітні технології, включаючи розподілені системи фільтрації трафіку, контроль перевантаження, чорні списки IP-адрес та поведінковий аналіз мережевого трафіку.

Категорія атак, яка не є характерною для моделі CIA, є атаки на обхід механізмів автентифікації та авторизації. Такі атаки спрямовані на подолання систем контролю доступу до інформаційних ресурсів та можуть призводити до порушення як конфіденційності, так і цілісності даних. До них належать атаки методом повного перебору, використання вкрадених облікових даних, експлуатація вразливостей у системах управління доступом тощо.

Нові види атак виникають і через розвиток ШІ та машинного навчання, спрямовані на компрометацію алгоритмів машинного навчання та систем на їх основі. До таких атак належать змагальні атаки, атаки з отруєнням, атаки через інверсію моделі, тощо. Такі атаки становлять серйозну загрозу для систем інформаційної безпеки, які базуються на технологіях штучного інтелекту, зокрема, систем виявлення вторгнень, систем аналізу аномалій та систем профілювання користувачів.

Ще один вид класифікації атак за механізмом впливу – поділ на атаки з використанням соціальної інженерії та суто технічні атаки. Атаки з використанням соціальної інженерії базуються на маніпуляції людським фактором та експлуатації психологічних особливостей людей. До таких атак належать фішинг, вішинг, претекстинг, баітинг, тощо. Технічні атаки, натомість, базуються на експлуатації технічних вразливостей інформаційних систем та не передбачають безпосередньої взаємодії з людьми. До них належать атаки на веб-додатки (Наприклад: SQL-ін'єкції, XSS, CSRF), атаки на мережеву інфраструктуру, експлуатація вразливостей у програмному забезпеченні.

Узагальнюючи різні підходи до класифікації атак за механізмом впливу, можна стверджувати, що комплексне розуміння механізмів здійснення

кібератак є необхідною умовою для розробки ефективних систем захисту корпоративних мереж. Така класифікація дозволяє не лише структурувати знання про загрози інформаційній безпеці, але й розробляти цільові контрзаходи, спрямовані на захист від конкретних типів атак.

2.3. Методичні підходи до виявлення та класифікації інцидентів інформаційної безпеки в мережах

Процес класифікації інцидентів зазвичай здійснюється на основі таких критеріїв, як джерело інциденту, механізм реалізаці, вплив на систему, а також ступінь критичності. У деяких випадках також враховується потенційна "ланцюгова реакція" – можливість того, що інцидент спричинить інші, вторинні інциденти або поглибить існуючі вразливості. Цей підхід особливо актуальний у великих розподілених системах, де взаємозалежність компонентів створює додатковий рівень складності в класифікації та пріоритезації подій. Такий підхід дозволяє структурувати масиви подій, які фіксуються у великих корпоративних мережах, зменшуючи навантаження на IRT (команду реагування на інциденти) та підвищуючи швидкість ухвалення рішень. Додатково можуть використовуватись інструменти автоматичного присвоєння пріоритетів на основі вагових коефіцієнтів, які враховують комбінацію кількох факторів: частота появи, вплив на критичні активи, можливість масштабування атаки тощо. Такий підхід дозволяє забезпечити баланс між швидкістю реагування та ефективністю розподілу ресурсів у команді безпеки.

У межах методичного аналізу також важливим є поділ процесів виявлення на проактивні та реактивні. Залучення даних з зовнішніх джерел, таких як репутаційні бази IP-адрес або IOC-індикатори, значно покращує точність раннього попередження та знижує кількість хибнопозитивних спрацювань.

2.3.1. Засоби виявлення та прогнозування інцидентів

Ускладнення кіберзагроз та підвищення рівня їх технологічності стимулюють впровадження комплексних підходів до виявлення та прогнозування інцидентів. У науковій літературі та практиці інформаційної безпеки виділяють кілька ключових засобів виявлення інцидентів, кожен з яких має свої особливості та сфери застосування.

Системи виявлення вторгнень, такі як IDS, є одним із найпоширеніших засобів виявлення інцидентів інформаційної безпеки в корпоративних мережах. Відповідно до класифікації, запропонованої Національним інститутом стандартів і технологій США (NIST), системи виявлення вторгнень поділяються на мережеві та хостові. Мережеві системи виявлення вторгнень функціонують на рівні мережевої інфраструктури та здійснюють аналіз мережевого трафіку з метою виявлення аномалій та потенційно небезпечних дій. Хостові системи, натомість, працюють на рівні окремих хостів та фокусуються на аналізі журналів подій, процесів, файлової системи та інших компонентів операційної системи.

За методологічним підходом до виявлення інцидентів системи IDS поділяються на системи, що базуються на сигнатурах, та системи, що базуються на виявленні аномалій. Сигнатурні системи використовують базу даних відомих шаблонів атак (сигнатур) та порівнюють з ними мережевий трафік або події в системі. Перевагою такого підходу є висока точність виявлення відомих атак, проте він неефективний для виявлення нових, раніше невідомих загроз та їх модифікацій.

Системи виявлення аномалій, у свою чергу, базуються на створенні моделі нормальної поведінки системи та виявленні відхилень від цієї моделі. Такий підхід дозволяє виявляти нові типи атак, проте характеризується вищим рівнем хибних спрацьовувань. Дослідження, проведені компанією “Gartner”, свідчать про те, що оптимальним є комбінований підхід, який поєднує сигнатурні методи та методи виявлення аномалій.

Розвитком концепції систем виявлення вторгнень є системи запобігання вторгненням, IPS зокрема, які не лише виявляють потенційні інциденти, але й автоматично вживають заходів для їх запобігання. Ефективність систем IPS суттєво залежить від точності алгоритмів виявлення та класифікації загроз, а також від рівня їх інтеграції з іншими компонентами системи інформаційної безпеки.

Одним із перспективних напрямів розвитку систем виявлення та прогнозування інцидентів є використання методів машинного навчання та штучного інтелекту. Системи машинного навчання для виявлення інцидентів безпеки можуть використовувати різноманітні алгоритми та підходи, включаючи нейронні мережі, метод опорних векторів, дерева рішень, алгоритми кластеризації тощо. Дослідження Корольова В.Ю. та Ходаківського В.М. демонструють, що глибокі нейронні мережі, зокрема, рекурентні нейронні мережі (RNN) та згорткові нейронні мережі (CNN), є особливо ефективними для аналізу мережевого трафіку та виявлення аномалій.

Тепер про проблеми інтерпретованості моделей. Чорні скриньки, такі як глибокі нейронні мережі, хоч і демонструють високу ефективність у виявленні загроз, проте ускладнюють процес аналізу причин спрацьовування та прийняття рішень щодо реагування на інциденти. Для вирішення цієї проблеми розробляються методи пояснюваного штучного інтелекту, які дозволяють отримувати інтерпретовані результати аналізу та пояснення прийнятих рішень. Тут варто згадати й системи управління інформацією та подіями безпеки. SIEM-системи забезпечують централізований збір, зберігання та аналіз журналів подій з різних джерел, включаючи мережеві пристрої, сервери, робочі станції, системи безпеки тощо. SIEM-системи використовують різноманітні методи аналізу даних, включаючи кореляцію подій, поведінковий аналіз, аналіз часових рядів тощо. Особливо перспективним напрямом розвитку SIEM-систем є впровадження методів машинного навчання для автоматизації процесів виявлення та класифікації інцидентів. Раніше згадані UEBA є ще одним

важливим засобом виявлення інцидентів, зокрема тих, що пов'язані з інсайдерськими загрозами.

У контексті прогнозування інцидентів інформаційної безпеки особливої уваги заслуговують системи аналізу загроз TIP. Такі системи забезпечують збір, аналіз та використання інформації про загрози з різних джерел, включаючи відкриті бази даних вразливостей, комерційні бази даних загроз, спеціалізовані форуми та соціальні мережі, дані від партнерів та власні дані організації. Окремим напрямом розвитку засобів виявлення та прогнозування інцидентів є використання технології приманок (їх називають: Honeypot, Honeynet). Такі системи імітують реальні інформаційні ресурси з метою приваблення зловмисників та вивчення їхніх методів та інструментів. Відповідно до дослідження Шнайдера Б. можна ствердити, що використання технології приманок дозволяє не лише виявляти нові типи загроз, але й отримувати цінну інформацію для прогнозування майбутніх атак.

Інтеграція різноманітних засобів виявлення та прогнозування інцидентів у єдину систему управління інформаційною безпекою є ключовим фактором підвищення ефективності захисту корпоративних мереж. Відповідно до концепції кібербезпеки нового покоління, запропонованої Хофманом Л. та Петерсоном К., оптимальним є підхід, який передбачає комплексне використання різних засобів виявлення та прогнозування інцидентів з урахуванням специфіки корпоративної мережі та бізнес-процесів організації.

2.3.2. Методичні інструменти моніторингу інцидентів

Відповідно до стандарту ISO/IEC 27035, моніторинг інцидентів є невід'ємною складовою процесу управління інцидентами та передбачає систематичне спостереження, аналіз та оцінювання стану інформаційної безпеки. Окрім безперервного моніторингу в реальному часі, важливим елементом є збереження історичних логів та здійснення постінцидентного аналізу. Це дозволяє не лише відтворити повну картину події, а й оновити

існуючі політики безпеки, враховуючи реальні сценарії загроз. Встановлення процедур аудиту журналів подій має бути закріплено на нормативному рівні, із зазначенням періодичності та відповідальних осіб.

Виділяють декілька ключових методичних інструментів моніторингу інцидентів у сучасній практиці інформаційної безпеки, кожен з яких має свої особливості та сфери застосування. Нижче наведено структуровану схему основних методичних інструментів, що застосовуються для моніторингу інцидентів інформаційної безпеки в корпоративних мережах. Схема охоплює засоби збору, аналізу та реагування на події безпеки з урахуванням сучасних технологій (рис. 2.5).

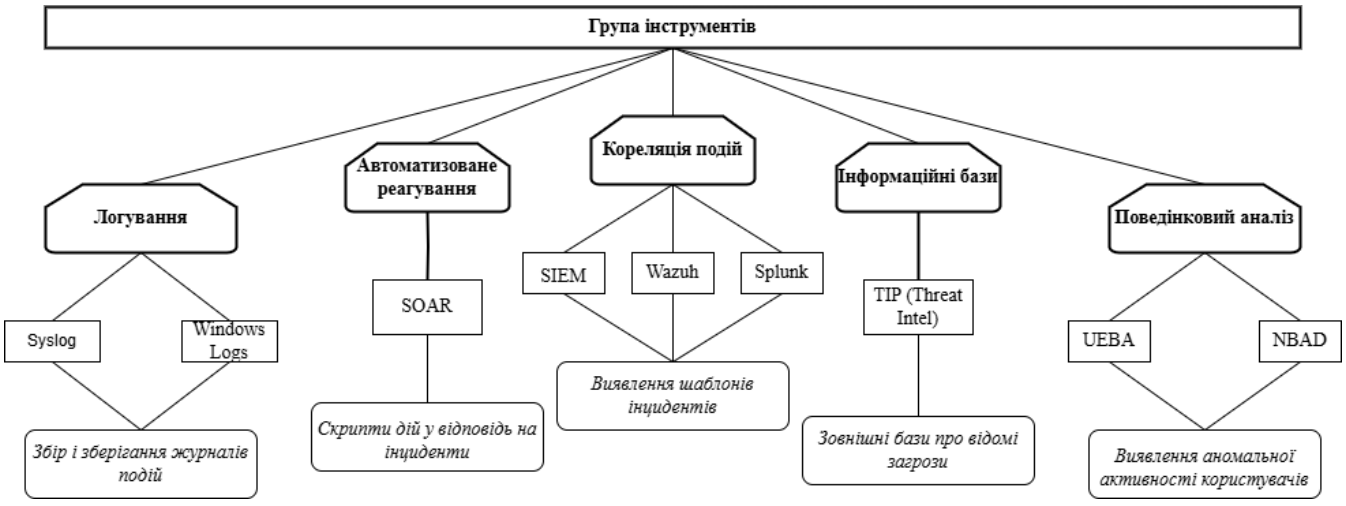

Рис. 2.5. Методичні інструменти моніторингу інцидентів

Одним із найпоширеніших підходів є використання індикаторів компрометації. Індикатори компрометації – це артефакти, які з високою ймовірністю свідчать про успішну атаку або спробу атаки на інформаційну систему. До таких індикаторів належать хеш-суми шкідливого програмного забезпечення, IP-адреси та доменні імена зловмисників, шаблони мережевого трафіку, характерні для атак, тощо. Ефективність використання індикаторів компрометації суттєво залежить від їх актуальності та повноти, а також від наявності механізмів автоматизованого обміну такими індикаторами між

різними організаціями та спільнотами. Для стандартизації формату представлення та обміну індикаторами компрометації розроблено спеціальні мови та протоколи, такі як (див. рис. 2.6.).

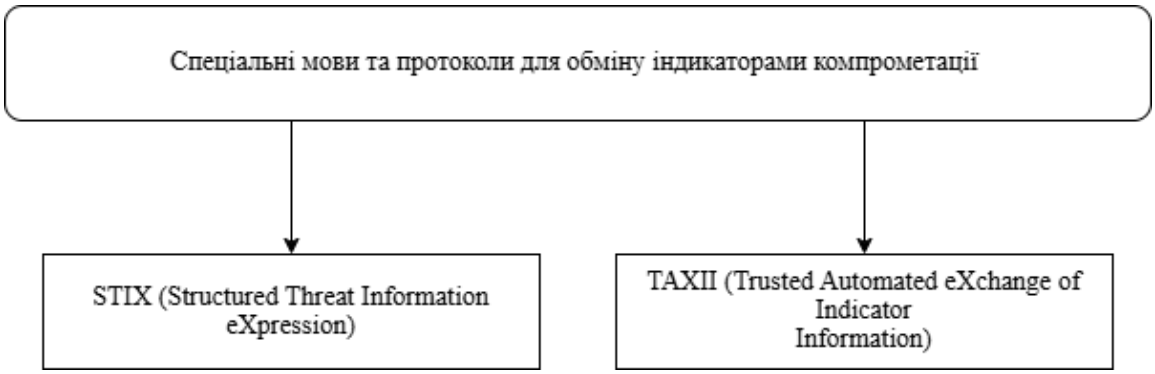

Рис. 2.6. Спеціальні мови та протоколи

Розвитком концепції індикаторів компрометації є індикатори атаки, які фокусуються не на артефактах успішної атаки, а на виявленні шаблонів поведінки, характерних для атакуючих на етапі підготовки та проведення атаки. Такий підхід дозволяє виявляти атаки на ранніх стадіях, до компрометації системи.

Концепція централізованого управління журналами подій передбачає збір, нормалізацію, зберігання та аналіз журналів подій з різних джерел у єдиному сховищі. Відповідно до досліджень Бурячка В.Л. та співавторів, централізоване управління журналами подій дозволяє не лише підвищити ефективність виявлення інцидентів, але й забезпечити можливість проведення розслідувань та відновлення хронології подій після інцидентів.

Візуалізація даних є теж не менш важливим методичним інструментом моніторингу інцидентів, який дозволяє представити складні взаємозв'язки між різними подіями та сутностями в зрозумілій для людини формі.

Системи візуалізації даних у сфері інформаційної безпеки використовують різноманітні графічні представлення, включаючи графіки часових рядів, теплові карти, графи зв'язків, географічні карти тощо. Особливо

ефективним є використання інтерактивних візуалізацій, які дозволяють користувачеві динамічно змінювати параметри відображення даних та здійснювати поглиблений аналіз окремих аспектів інцидентів. Подальший розвиток цих систем спрямований на інтеграцію з алгоритмами штучного інтелекту. Такий симбіоз автоматизованого аналізу з інтуїтивно зрозумілим інтерфейсом суттєво покращує здатність до виявлення прихованих або багатоступеневих атак.

Моніторинг мережевого трафіку – ще один ключовий елемент систем виявлення загроз. За допомогою аналізу трафіку можливо виявити до 70% зовнішніх атак. Такий аналіз охоплює як метадані пакетів (заголовки, протоколи, маршрути), так і їхнє безпосереднє навантаження. Надзвичайно ефективно себе проявляють технології глибокого аналізу пакетів DPI, що дозволяють не лише ідентифікувати відомі зразки шкідливого коду, але й виявляти спроби експлуатації вразливостей, несанкціоновану передачу даних тощо. DPI дозволяють здійснювати детальний аналіз змісту мережевих пакетів та виявляти шкідливий код, ознаки експлуатації вразливостей, витік конфіденційної інформації тощо.

Моніторинг інцидентів інформаційної безпеки: окремо уваги заслуговують системи моніторингу в реальному часі, забезпечують безперервний аналіз подій та генерацію сповіщень про потенційні інциденти з мінімальною затримкою. Такі системи є особливо важливими для своєчасного виявлення та реагування на критичні інциденти, які можуть призвести до значних збитків.

До того ж не менш важливий аспект моніторингу інцидентів інформаційної безпеки – автоматизація процесів виявлення, класифікації та реагування на інциденти. Організації, які активно використовують автоматизацію в процесах управління інцидентами, демонструють на 70% вищу ефективність реагування на інциденти порівняно з організаціями, які покладаються переважно на ручні процеси.

SOAR-платформи забезпечують інтеграцію різноманітних інструментів безпеки, автоматизацію рутинних завдань та координацію дій різних команд у процесі реагування на інциденти. Відповідно до даних з досліджень компанії “Gartner”, впровадження SOAR-рішень дозволяє скоротити час реагування на інциденти на 80% та зменшити навантаження на фахівців з інформаційної безпеки на 50%.

Існубть також методи проактивного моніторингу, які фокусуються на виявленні потенційних загроз до їх реалізації. До таких методів належать сканування вразливостей, аналіз конфігурацій, перевірка на відповідність стандартам безпеки, тестування на проникнення тощо. Проактивний моніторинг дозволяє запобігти до 75% інцидентів інформаційної безпеки.

Особливого значення набуває інтеграція різноманітних методичних інструментів моніторингу інцидентів у єдину систему управління інформаційною безпекою. Такий підхід дозволяє забезпечити комплексний захист корпоративних мереж та ефективне реагування на інциденти різних типів. Відповідно до концепції адаптивної архітектури безпеки, запропонованої компанією “Gartner”, ефективна система моніторингу інцидентів має включати інструменти для профілактики, виявлення, реагування та прогнозування інцидентів, а також забезпечувати постійне вдосконалення процесів на основі зворотного зв'язку та аналізу досвіду реагування на попередні інциденти.

Узагальнюючи різні підходи до моніторингу інцидентів інформаційної безпеки, можна стверджувати, що оптимальним є використання комплексу методичних інструментів, адаптованих до конкретних потреб та особливостей організації. Такий підхід дозволяє забезпечити високий рівень захисту корпоративних мереж та ефективне реагування на інциденти різних типів.

2.4. Автоматизація класифікації інцидентів інформаційної безпеки в мережах

Процеси автоматизованої класифікації передбачають не лише розподіл інцидентів за типами, джерелами чи рівнем критичності, але й побудову відповідної логіки ескалації, контекстної інтерпретації подій та рекомендацій щодо реагування. Ключовими інструментами в цьому процесі є експертні системи і моделі штучного інтелекту, що дає змогу підвищити точність, швидкість і адаптивність управління інцидентами.

Одним із найважливіших напрямків розвитку автоматизації є застосування контекстної класифікації. У цьому випадку система враховує не лише сам факт події, а й її зв’язок з іншими обставинами: наприклад, поведінку користувача, історію доступу до об’єктів, час доби, використання нетипового пристрою чи геолокацію. Такий підхід дозволяє істотно зменшити кількість хибнопозитивних спрацювань і спрямувати ресурси безпеки на аналіз дійсно нетипових ситуацій.

У різних компаніях можуть бути різні рівні ризик-апетиту, критичність активів, специфіка операційної діяльності, тому автоматизовані системи мають підтримувати можливість створення кастомних шаблонів класифікації, адаптованих до внутрішніх вимог. Це особливо важливо в умовах динамічного змінення внутрішнього та зовнішнього середовища, коли типові шаблони класифікації можуть втрачати актуальність або виявлятись недостатньо гнучкими. Наприклад, компанії, що працюють у сфері фінансів, матимуть зовсім інший профіль загроз порівняно з виробничими чи освітніми установами, тому ефективність автоматизованих систем значною мірою залежить від їх здатності враховувати галузеві особливості та сценарії. Відповідно, механізми адаптації класифікаційних моделей повинні охоплювати можливість внесення змін без необхідності повного перенавчання або технічної реконфігурації системи.

Більш того, процеси кастомізації мають бути максимально зручними для кінцевих користувачів – аналітиків безпеки, операторів SOC або адміністраторів – і не вимагати глибокого втручання у внутрішню логіку роботи системи. Це може реалізовуватись через візуальні редактори сценаріїв класифікації, системи правил на основі фреймворків типу MITRE ATT&CK, або динамічні фільтри, які дозволяють налаштовувати порогові значення для кожного типу події.

2.4.1. Експертні системи аналізу інцидентів

Експертні системи в контексті інформаційної безпеки – це програмні комплекси, що реалізують знання і логіку дій фахівця-аналітика, ґрунтуючись на наперед заданих правилах, шаблонах і базах знань. Такі системи формуються на основі глибокого аналізу типових інцидентів, сценаріїв розвитку атак, індикаторів компрометації та оперативних політик реагування. Базово архітектура експертної системи має структуру, як на рис. 2.7.

Рис. 2.7. Типова архітектура експертної системи

Однією з найпоширеніших форм експертної класифікації є правила на основі логіки IF-THEN, де на основі певної комбінації параметрів (наприклад, поєднання типу події, джерела IP, кількості повторів тощо) інциденту присвоюється визначена категорія.

Проте їх основним обмеженням є статичність – у разі появи нових або складно комбінованих загроз система не здатна до самостійного узагальнення або навчання. Крім того, ефективність таких систем суттєво залежить від повноти бази знань, яка потребує постійної підтримки з боку досвідчених фахівців.

У SOC-центрах експертні системи застосовуються як перший рівень класифікації – для фільтрації та категоризації масових, часто повторюваних подій. Більш складні інциденти або випадки з нестандартною поведінкою потребують залучення гнучкіших засобів аналізу – зокрема, моделей штучного інтелекту.

Разом із цим, дедалі частіше реалізуються гібридні підходи, що поєднують експертні системи із адаптивними модулями аналізу на основі машинного навчання. Така комбінація дозволяє компенсувати недоліки жорстких логічних конструкцій шляхом постійного збагачення системи новими правилами, виведеними на основі виявлених закономірностей. Наприклад, модель на базі дерева рішень може бути інтегрована з експертною платформою як допоміжний механізм уточнення категорії інциденту.

Крім того, експертні системи можуть бути використані не лише для класифікації, але й для генерації рекомендацій, тобто автоматизованих пропозицій щодо дій у відповідь. Це особливо актуально для сценаріїв, де час на прийняття рішення обмежений, а участь людини – мінімальна. Наприклад, у разі виявлення шаблону активності, подібного до попередньо зафіксованого інциденту, система здатна не лише ідентифікувати загрозу, але й викликати заздалегідь визначений механізм реагування – повідомлення, блокування сесії, або ізоляцію сегменту мережі.

На практиці доцільно впроваджувати багаторівневу структуру використання експертних систем, де на кожному рівні функціонує окремий тип логіки: від простих шаблонів (наприклад, кількість запитів до одного порту за одиницю часу) до складних сценаріїв з аналізом послідовності подій, джерел, об'єктів доступу та взаємодії з іншими компонентами інфраструктури.

Таким чином, попри обмеження, експертні системи залишаються ефективним інструментом у комплексній архітектурі кіберзахисту, особливо в тих випадках, коли потрібна прозорість, повторюваність рішень і стабільність роботи навіть за умов недостатньої кількості навчальних даних.

2.4.2. Використання штучного інтелекту для розпізнавання інцидентів

Застосування алгоритмів ШІ у сфері інформаційної безпеки розширює можливості систем не лише для класифікації, а й для адаптивного виявлення нових типів інцидентів, побудови контексту подій та автоматичної оцінки ризиків. На відміну від традиційних систем, які покладаються на фіксовані правила, ШІ-моделі здатні виявляти приховані залежності між подіями, ідентифікувати аномальні шаблони поведінки та вчитися з історичних даних. Здебільшого ШІ використовують у класифікації подій за контекстом події (на основі її логів, системних повідомлень, запитів HTTP, тощо) та кластеризації інцидентів для виявлення нових загроз або ж груп загроз. Наприклад, застосування нейронних мереж до аналізу логів дозволяє виявляти складні послідовності, які є характерними для багатоступеневих атак типу APT. Один із поширених методів – LSTM-мережі, які використовуються для обробки логів як часових послідовностей. Доволі часто використовують ШІ і для предиктивної аналітики. Предиктивна аналітика об’єднує в собі оцінку ймовірності виникнення загрози та оцінку масштабу цієї загрози. Автоматизоване ранжування подій за рівнем критичності теж є тим напрямком, де застосування ШІ лежить в основі на сьогодні. Один з таких прикладів застосування є NLP до

аналізу повідомлень журналів та описів інцидентів. Завдяки цьому можлива автоматизована інтерпретація, категоризація та узагальнення подій навіть без чіткої структури у вихідних даних. На практиці впровадження таких систем здебільшого відбувається рамках SIEM-платформ з ML-модулями, такими як “IBM QRadar” чи “Azure Sentinel”.

Попри свою інноваційність та максимальну продуктивність, такі моделі все одно мають низку проблем та недоліків у сфері інформаційної безпеки. Такі моделі потребують великих обсягів навчальних даних та матеріалу, які мають мають бути максимально якісними. Доволі часто ще виникає потреба в регулярному перенавчанні моделей, особливо це необхідно в умовах динамічно-змінних ситуаціях із високим ступенем небезпеки. До того ж, результати обробки такої моделі можуть бути важко інтерпретованими, що у свою чергу ускладнює аудит і прийняття рішень.

У випадках, коли критично важливо мати змогу обґрунтувати та пояснити логіку дій системи – наприклад, під час розслідування інциденту або в процесі зовнішнього аудиту – так звана «непрозорість» моделей ШІ може стати серйозним бар’єром. Ця проблема відома як «black-box effect», коли навіть розробники систем не можуть точно описати, чому модель класифікувала певну подію як критичну чи звичайну.

Інша важлива проблема полягає в тому, що дані, на яких навчається модель, можуть бути нерівномірно представленими або недостатньо різноманітними, що в окремих випадках спричиняє викривлення результатів – наприклад, надмірну увагу до певних типів подій і недостатню чутливість до інших, не менш критичних сценаріїв. Наприклад, якщо навчальна вибірка містить переважно приклади зовнішніх атак, система може не виявляти внутрішні загрози належним чином. Подолання цього ефекту вимагає ретельної роботи з підготовкою та включення репрезентативних інцидентів із періодичного аудиту точності моделі на реальних даних.

Крім того, слід брати до уваги вразливість самих моделей ШІ до атак, таких як adversarial input – навмисно змінені дані, які можуть «обманути»

модель та змусити її зробити помилкові висновки. Це створює потребу у впровадженні додаткових механізмів перевірки або резервного ручного перегляду рішень у критичних випадках.

З огляду на вище сказане, можна ствердити, що ефективною практикою є комбіноване використання експертних систем і ШІ-моделей, де перші відповідають за стабільні, перевірені сценарії, а другі – за адаптацію до нових, невизначених загроз.

Висновок до розділу 2

Проаналізовано та досліджено, що методичні підходи до виявлення та класифікації інцидентів інформаційної безпеки мають ключове значення для підвищення рівня кіберзахисту організацій. Різноманітність форм загроз, складність сучасних атак, а також швидкість їх розповсюдження вимагають гнучких, масштабованих і адаптивних систем виявлення, здатних реагувати на події в реальному часі.

Класифікація загроз на основі різних критеріїв – від джерела та вектора атаки до її наслідків – є важливою передумовою для вибору оптимальних заходів реагування. Водночас, просте визначення типу інциденту без урахування контексту його реалізації є недостатнім для ефективного реагування. Саме тому сучасні рішення все більше тяжіють до використання поведінкових моделей, аналітики аномалій, машинного навчання та кіберрозвідки, що дозволяє будувати захист не лише реактивного, а й проактивного характеру.

Таким чином, можна стверджувати, що методична база управління інцидентами повинна ґрунтуватися на поєднанні класичних принципів інформаційної безпеки із сучасними технологічними можливостями. Це дозволить забезпечити не лише виявлення загроз на ранніх етапах, а й підвищити якість аналізу, пріоритезацію ризиків та ефективність дій з боку команд реагування. Одержані результати створюють підґрунтя для прикладної

частини дослідження, яка зосередиться на розробці рекомендацій та практичному застосуванні засобів виявлення і класифікації інцидентів у реальних умовах корпоративних мереж.

Розділ 3 ДОСЛІДЖЕННЯ І РОЗРОБКА РЕКОМЕНДАЦІЙ ПО ВИКОРИСТАННЮ ЗАСОБІВ ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ МЕРЕЖАХ

У цьому розділі здійснюється аналіз практичного застосування сучасних засобів виявлення та класифікації інцидентів інформаційної безпеки в контексті корпоративних мереж. Розгляд зосереджено як на існуючих технічних рішеннях, так і на підходах до їх інтеграції в структуру інформаційної безпеки організації. Особливу увагу приділено оцінці ефективності використання SIEM-систем, модулів UEBA, інструментів аналізу мережевого трафіку та зовнішніх джерел Threat Intelligence.

Основний акцент зроблено на дослідженні реальних можливостей технічних засобів у контексті їх ефективності, масштабованості та придатності до інтеграції в існуючу інфраструктуру безпеки організації. Також у межах розділу розроблено низку практичних рекомендацій, які можуть бути використані організаціями для вдосконалення наявних механізмів кіберзахисту. Вони базуються на принципах побудови гнучких та адаптивних систем, здатних швидко реагувати на зміну загрозової обстановки, виявляти нові типи аномальної активності та ефективно взаємодіяти з іншими елементами архітектури інформаційної безпеки.

3.1. Приклад використання засобів виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах

Впровадження комплексних рішень із виявлення та класифікації інцидентів інформаційної безпеки потребує системного підходу та врахування специфіки конкретної корпоративної мережі. Ефективність таких рішень суттєво залежить від їх адаптованості до бізнес-процесів та IT-інфраструктури

організації. Нижче зведена порівняльна таблиця ефективності засобів виявлення для таких цілей (див. табл. 3.1).

Таблиця 3.1.

Порівняльна характеристика засобів виявлення інцидентів

Засіб	Точність	Швидкість	Інтеграція	Особливості
IDS	Середня	Висока	Легка	Працює за сигнатурами
IPS	Висока	Середня	Середня	Автоматично блокує загрози
SIEM	Висока	Низька	Складна	Кореляція подій з усієї системи
UEBA	Висока	Змінна	Складна	Аналіз поведінки

Розглянемо приклад імплементації інтегрованої системи виявлення та класифікації інцидентів в умовах великої фінансової установи з розгалуженою корпоративною мережею. Дана організація має центральний офіс та 15 регіональних відділень, об'єднаних корпоративною мережею з гібридною інфраструктурою, що включає як локальні обчислювальні ресурси, так і хмарні сервіси. Щоденний обсяг мережевого трафіку становить приблизно 5 ТБ, а кількість активних користувачів – понад 2000. За таких умов створення ефективної системи виявлення та класифікації інцидентів інформаційної безпеки є критично важливим завданням.

На першому етапі впровадження було проведено комплексний аудит існуючої інфраструктури та систем безпеки. Це дозволило виявити наявні прогалини та визначити ключові вектори потенційних атак. Керуючись цим принципом, було здійснено детальне картографування мережі з визначенням критичних активів та потенційних вразливостей. Архітектура розробленої системи базується на багаторівневому підході до виявлення інцидентів, що поєднує різноманітні методології та інструменти. На рівні периметру мережі було розгорнуто комплекс систем виявлення вторгнень – IDS та систем запобігання вторгненням – IPS, доповнених сучасними фаєрволами нового

покоління з функціями глибокого аналізу пакетів. Внутрішня мережа захищена сегментацією через запровадження віртуальних локальних мереж з диференційованими політиками доступу. Така структура забезпечує контроль як зовнішніх, так і внутрішніх загроз.

Центральним елементом впровадженої системи став SIEM-комплекс, що агрегує дані з усіх компонентів інфраструктури. Згідно з рекомендаціями ISO/IEC 27035, збір та кореляція подій із різноманітних джерел є необхідною умовою ефективного виявлення інцидентів інформаційної безпеки. Логування здійснюється для всіх критичних систем, включаючи серверні платформи, мережеве обладнання, системи автентифікації та авторизації, бази даних та прикладне програмне забезпечення. Інтеграція SIEM з Active Directory дозволила реалізувати контекстний аналіз поведінки користувачів та виявляти аномалії, пов'язані з потенційними інсайдерськими загрозами.

Впроваджена система використовує багаторівневий механізм класифікації інцидентів. На першому рівні відбувається категоризація за джерелом загрози. На другому – за типом атаки: DDoS, фішинг, шкідливе програмне забезпечення, несанкціонований доступ тощо. На третьому – за рівнем критичності. Критичність інциденту визначається на основі комплексного аналізу, що враховує цінність атакованих активів, потенційний вплив на бізнес-процеси та можливі репутаційні і фінансові наслідки.

Особливістю впровадженої системи є інтеграція традиційних механізмів виявлення, базованих на сигнатурах, з передовими алгоритмами машинного навчання. Кузнєцов М.Ю. та співавтори у дослідженні “Методи підвищення інтерпретованості моделей машинного навчання для задач кібербезпеки. Інформаційна безпека держави, суспільства та особистості” наголошують на важливості використання інтерпретованих моделей при виявленні аномалій у корпоративних мережах, оскільки розуміння логіки прийняття рішень алгоритмом має критичне значення для оперативної реакції на інциденти та мінімізації хибнопозитивних спрацювань. У рамках описаної системи було

впроваджено гібридну модель, що поєднує дерева рішень та нейронні мережі для класифікації мережевих аномалій.

Аналіз мережевого трафіку здійснюється за допомогою системи глибокого аналізу пакетів, що дозволяє ідентифікувати аномальну активність навіть у шифрованому трафіку через аналіз метаданих та статистичних характеристик потоків. Для виявлення розподілених атак використовується технологія поведінкового аналізу, що дозволяє агрегувати та корелювати події з різних сегментів мережі. Така інтеграція різноманітних підходів забезпечує комплексне покриття широкого спектру загроз.

Ефективність впровадженої системи підтверджується скороченням середнього часу виявлення інциденту з 4.5 годин до 22 хвилин, а також зменшенням кількості хибнопозитивних спрацювань на 78%. Протягом перших шести місяців експлуатації система дозволила виявити та нейтралізувати 17 критичних інцидентів, включаючи цілеспрямовану фішингову кампанію, спробу впровадження шкідливого програмного забезпечення через компрометацію облікових записів постачальників та аномальну активність користувачів, пов'язану з несанкціонованим доступом до конфіденційної інформації.

У межах дослідження було проаналізовано роботу умовного підприємства з чисельністю до 100 працівників, яке впровадило SIEM-рішення на базі Wazuh та ELK Stack. Основна мета – централізований збір логів, виявлення потенційних атак, а також фіксація подій входу й спроб ескалації привілеїв. На практиці вдалося виявити декілька підозрілих спроб входу з невідомих IP-адрес до облікового запису адміністратора. Після аналізу логів та кореляції подій було встановлено, що облікові дані могли бути скомпрометовані через фішингову кампанію. Реакцією було обмеження доступу, примусова зміна пароля та оновлення політик MFA. Таким чином, навіть базове впровадження SIEM на безкоштовному стеку дало змогу виявити інцидент до його ескалації.

Інший приклад стосується компанії, що використовує UEBA-модулі на базі Microsoft Defender for Endpoint у поєднанні з Azure AD. Після тривалого моніторингу поведінки користувачів система зафіксувала аномалію: працівник віддалено підключився до мережі з геолокації, яка не відповідала його звичному місцю роботи, і через кілька хвилин ініціював перенесення великих обсягів даних на зовнішній ресурс. Завдяки поведінковому аналізу, інцидент був визначений як критичний згідно з внутрішніми політиками безпеки. Підозрілі дії виявилися результатом компрометації акаунту, доступ до якого було отримано через фішинг. Це демонструє перевагу UEBA над традиційними рішеннями – система не потребувала сигнатури, а реагувала саме на поведінкову аномалію.

Практика показала, що найбільш ефективною є інтеграція автоматизованих систем виявлення з процесами безперервного моніторингу, які виконуються кваліфікованими фахівцями. Залучення людського експертного аналізу дозволяє виявляти складні багатоетапні атаки, які можуть залишатися непоміченими автоматизованими системами через їх нестандартні патерни.

3.2. Рекомендації по використанню засобів виявлення та класифікації інцидентів інформаційної безпеки в корпоративних мережах

Першочерговою рекомендацією є забезпечення комплексності підходу. Комплексність передбачає не лише технологічну інтеграцію різноманітних систем виявлення та аналізу, але й узгодженість організаційних процесів, пов'язаних із реагуванням на інциденти. Стандарт ISO/IEC 27035 визначає п'ять основних етапів управління інцидентами: планування та підготовка, виявлення та звітування, оцінка та прийняття рішення, реагування, напрацювання висновків. Реалізація цього циклу потребує координації дій різних підрозділів організації. Систематизоване уявлення про реалізацію ефективного процесу виявлення інцидентів дозволяє сформувати послідовність кроків, які доцільно

врахувати організаціям під час впровадження відповідних рішень. Їх узагальнено представлено на рис. 3.1.

Рис. 3.1. Рекомендована послідовність дій з впровадження засобів виявлення інцидентів ІБ у корпоративних мережах

Налаштування систем виявлення інцидентів з урахуванням специфічних характеристик конкретної корпоративної мережі дуже важливий аспект. Універсальні шаблонні правила та політики часто виявляються неефективними через особливості бізнес-процесів та інфраструктури організації. У зв'язку з цим рекомендується проведення попереднього періоду спостереження за нормальною активністю в мережі для встановлення базових паттернів та подальшого налаштування порогових значень для детектування аномалій.

Пріоритезація критичних активів та аналіз ризиків мають стати основою для побудови стратегії виявлення інцидентів. Обмеженість ресурсів, доступних

для забезпечення інформаційної безпеки, зумовлює необхідність їх оптимального розподілу з фокусом на найбільш критичні компоненти інфраструктури. Проведення детального аналізу ризиків дозволяє ідентифікувати активи, захист яких потребує першочергової уваги, та зосередити на них найбільш просунуті механізми моніторингу та виявлення інцидентів.

Інтеграція функціональності UEBA у систему виявлення інцидентів дозволяє суттєво підвищити її ефективність у контексті виявлення інсайдерських загроз та компрометації облікових записів. Це особливо важливо в умовах зростання кількості атак із застосуванням викрадених легітимних облікових даних. Такі інциденти зазвичай залишаються непоміченими для класичних систем контролю доступу, але можуть бути виявлені через аналіз нетипової активності – наприклад, зміни часових шаблонів, доступу до незвичних ресурсів або аномального обсягу дій протягом короткого періоду. Саме UEBA здатна підхопити ці «поведінкові сигнали» та оперативно попередити потенційне вторгнення. Технології UEBA забезпечують створення поведінкових профілів користувачів та систем, що дозволяє виявляти відхилення від нормальної поведінки навіть у випадках, коли зловмисник використовує легітимні облікові дані та не порушує формальних політик безпеки.

Забезпечення багаторівневої системи класифікації інцидентів є важливою рекомендацією. Саме таке забезпечення повинне враховувати не лише технічні характеристики атаки, але й потенційний вплив на бізнес-процеси організації. Така система класифікації має бути інтегрована з процесами реагування та забезпечувати автоматизоване визначення пріоритетності інцидентів на основі їх критичності. ISO/IEC 27035 рекомендує включати до системи класифікації такі параметри, як тип інциденту, джерело загрози, вектор атаки, цільові активи та потенційний вплив.

Використання технологій штучного інтелекту та машинного навчання суттєво розширює можливості систем виявлення інцидентів, особливо в

контексті виявлення невідомих раніше загроз та складних багатоетапних атак. Однак впровадження таких технологій потребує виваженого підходу та врахування проблем, пов'язаних з інтерпретованістю моделей та можливістю їх адаптації до змін у мережевому середовищі. Рекомендується використовувати гібридні підходи, що поєднують традиційні методи виявлення, базовані на правилах та сигнатурах, з алгоритмами машинного навчання, що дозволяє забезпечити баланс між точністю виявлення відомих загроз та здатністю ідентифікувати нові типи атак.

Інший фактор ефективності систем виявлення інцидентів – забезпечення їх масштабованості та продуктивності в умовах високих навантажень. Зростання обсягів мережевого трафіку та кількості пристроїв у корпоративних мережах створює значні виклики для систем моніторингу та аналізу. Архітектура сучасних систем виявлення інцидентів має забезпечувати можливість горизонтального масштабування та розподіленої обробки даних для ефективного функціонування в умовах великих корпоративних мереж. Рекомендується використання розподілених архітектур з можливістю балансування навантаження та забезпечення стійкості критичних компонентів.

Механізми контролю цілісності та узгодженості даних безпеки теж заслуговують чималої уваги. Маніпуляції з журналами подій та іншими джерелами даних є поширеною тактикою зловмисників для приховування слідів атаки. Впровадження механізмів криптографічного захисту цілісності даних та використання розподілених систем зберігання з механізмами консенсусу дозволяє мінімізувати ризики, пов'язані з компрометацією джерел інформації про інциденти.

Регулярне тестування ефективності систем виявлення інцидентів є необхідною умовою забезпечення їх актуальності в умовах еволюції загроз. Такі механізми, як red teaming, penetration testing та simulated attacks, дозволяють ідентифікувати прогалини у системі виявлення та вносити відповідні корективи. Безперервне вдосконалення систем виявлення інцидентів на основі результатів практичного тестування є ключовим елементом

забезпечення їх ефективності в довгостроковій перспективі – зазначають Бурячок В.Л. та співавтори. Реалізація програми підвищення обізнаності користувачів у питаннях інформаційної безпеки суттєво посилює загальну ефективність системи виявлення інцидентів. Користувачі, які володіють базовими знаннями щодо типових ознак кібератак, здатні виступати додатковим рівнем захисту, своєчасно повідомляючи про підозрілу активність. ISO/IEC 27035 підкреслює важливість залучення персоналу до процесів виявлення та реагування на інциденти через чітко визначені процедури ескалації та повідомлення про потенційні загрози.

Автоматизація процесів реагування на типові інциденти дозволяє суттєво скоротити час від виявлення до нейтралізації загрози. Технології SOAR забезпечують інтеграцію систем виявлення інцидентів з механізмами автоматичного реагування, що дозволяє реалізувати попередньо визначені сценарії нейтралізації типових загроз без безпосередньої участі фахівців з інформаційної безпеки. Автоматизація реагування на інциденти є критичним елементом сучасних систем інформаційної безпеки, особливо в контексті атак, що розвиваються зі швидкістю, яка перевищує можливості ручного реагування. Для організацій, що працюють у регульованих галузях або обробляють персональні дані, відповідність таким стандартам, як ISO/IEC 27001, може бути обов'язковою умовою. Впровадження систем виявлення інцидентів має враховувати вимоги цих стандартів щодо моніторингу, документування та звітності.

Кожен інцидент, незалежно від його критичності, повинен бути детально проаналізований та задокументований для виявлення факторів, що сприяли його виникненню, та визначення заходів щодо запобігання подібним інцидентам у майбутньому. Такий підхід відповідає концепції «извлечения уроков», визначеній в ISO/IEC 27035 як обов'язковий етап циклу управління інцидентами.

Забезпечення візуалізації та аналітичного представлення даних про інциденти значно підвищує ефективність роботи фахівців з інформаційної

безпеки. Розвинуті дашборди та аналітичні інструменти дозволяють оперативно ідентифікувати тренди та кореляції між різними подіями безпеки, що є критично важливим для виявлення складних багатоетапних атак. Візуалізація даних безпеки є не просто зручним інструментом, а необхідною умовою ефективного аналізу в умовах великих обсягів даних, характерних для сучасних корпоративних мереж.

Інтеграція зовнішніх джерел інформації про загрози у систему виявлення інцидентів дозволяє суттєво розширити її можливості щодо ідентифікації цілеспрямованих атак та нових типів загроз. До таких зовнішніх джерел належать як відкриті бази даних індикаторів компрометації, так і комерційні платформи кіберрозвідки, які надають аналітику з урахуванням галузевої специфіки. Поєднання внутрішніх логів з даними ззовні забезпечує багатоконтекстне бачення подій і дає змогу ефективніше виявляти скоординовані атаки, що розгортаються в кілька етапів. Зокрема, це має значення при виявленні APT-груп, які використовують легітимні інструменти для маскування шкідливої активності. Використання даних про індикатори компрометації, тактики, техніки та процедури, характерні для певних груп зловмисників, дозволяє реалізувати проактивний підхід до виявлення загроз. Інтеграція актуальних даних «threat intelligence» є невід'ємним елементом сучасних систем виявлення та класифікації інцидентів, що дозволяє ідентифікувати цілеспрямовані атаки на ранніх стадіях їх розвитку.

Розробка та підтримка плану реагування на інциденти є ключовою рекомендацією. Успішна реалізація заходів реагування передбачає не лише наявність технічних засобів і кваліфікованого персоналу, а й чітку регламентацію послідовності дій. У міжнародній практиці, зокрема в рамках стандарту ISO/IEC 27035, визначено п’ять ключових етапів реагування, які дозволяють забезпечити системність, керованість та ефективність цього процесу. Вони охоплюють усі критично важливі фази – від попередньої підготовки до навчання на основі помилок. Візуалізація цих етапів подана на рис. 3.2. Така розробка повинна визначати ролі та відповідальності всіх

задіяних підрозділів, процедури ескалації та комунікації, а також конкретні дії для різних типів інцидентів. План має регулярно оновлюватися та тестуватися через проведення симуляцій і навчань для забезпечення його актуальності та готовності персоналу до реагування на реальні загрози.

Рис. 3.2. Етапи впровадження реагування на інциденти

Окрім цього, важливо передбачити створення централізованого реєстру інцидентів, в якому відображатимуться всі зафіксовані події з детальним описом, часом виявлення, рівнем критичності, а також вжитими заходами реагування. Такий реєстр дозволяє здійснювати ретроспективний аналіз подій, виявляти закономірності та вдосконалювати політики безпеки на основі емпіричних даних. Регулярне тестування плану, зокрема через сценарні тренування, сприяє підвищенню обізнаності персоналу та зменшує ризики хаотичного реагування в реальній кризовій ситуації.

Висновок до розділу 3

Досліджено, що впровадження засобів виявлення та класифікації інцидентів має вирішальне значення для забезпечення комплексної безпеки корпоративної мережевої інфраструктури. Практичний аналіз засвідчив, що окремі технічні рішення, як-от SIEM та UEBA, за умови правильної конфігурації та постійної підтримки, здатні забезпечити як широкий спектр виявлення загроз, так і гнучку реакцію на інциденти в режимі реального часу.

Рекомендації, запропоновані в цьому розділі, передбачають не лише вибір конкретних технічних засобів, але й формування цілісної стратегії безпеки, яка включає побудову ефективної команди реагування, визначення пріоритетів на основі ризик-орієнтованого підходу, застосування стандартів обміну інформацією про загрози (наприклад, STIX/TAXII), а також впровадження етапного плану розвитку інструментів безпеки.

Крім того, важливим фактором є забезпечення взаємодії між різними компонентами системи захисту, їх інтеграція у загальну архітектуру IT-інфраструктури та поступове формування централізованої платформи управління інцидентами. Таким чином, ефективне використання засобів виявлення інцидентів має спиратися не лише на технічну досконалість інструментів, але й на системність у впровадженні, наявність підготовленого персоналу та готовність організації адаптуватися до змін у зовнішньому середовищі загроз.

Окремо підкреслюється значення гнучкості: швидка адаптація системи безпеки до нових загроз, масштабування засобів виявлення відповідно до зростання інфраструктури, а також динамічне оновлення політик реагування згідно з сучасними сценаріями атак. Такі фактори визначають життєздатність моделі кіберзахисту в довгостроковій перспективі.

Таким чином, запропоновані у цьому розділі практичні рекомендації можуть слугувати орієнтиром для організацій, що прагнуть підвищити рівень

безпеки своєї системи ІБ, рухаючись від фрагментарного реагування до комплексного, інтегрованого підходу, заснованого на принципах безперервного вдосконалення.

ВИСНОВКИ

1. Проаналізовано сучасний стан нормативно-правового забезпечення в Україні. Опрацьований матеріал засвідчив, що попри наявність базових регуляторних документів, значна частина вимог до реагування на інциденти є або фрагментарною, або декларативною, особливо в приватному секторі. Відсутність чітко унормованих механізмів взаємодії між державними та комерційними структурами істотно знижує загальний рівень кіберстійкості корпоративних систем.

2. Виокремлено ключові технічні, організаційні та кадрові проблеми, на основі вивчення наукових джерел та галузевих звітів, що ускладнюють ефективне реагування на інциденти. Зокрема, йдеться про фрагментарність впровадження SIEM-рішень, недостатню автоматизацію процесів класифікації, низький рівень міжсистемної інтеграції засобів захисту, а також обмежену кількість кваліфікованих фахівців. Ці чинники зумовлюють суттєве збільшення часу виявлення інцидентів і призводять до значних операційних ризиків.

3. Проведено аналіз актуальних загроз корпоративному середовищу, систематизовано методи поведінкового аналізу UEBA, виявлення аномалій у мережевому трафіку, методів автоматизованої класифікації інцидентів із використанням експертних систем та технологій штучного інтелекту. Обґрунтовано доцільність застосування комбінованого підходу, який об’єднує правила, основані на логіці IF–THEN, з адаптивними можливостями алгоритмів машинного навчання, що підвищує точність, швидкість і гнучкість реагування.

4. Проаналізовано та розроблено рекомендації відповідно до практичного розділу ефективність реалізації багаторівневої системи виявлення інцидентів у корпоративній мережі великої фінансової установи. Впроваджене рішення, що поєднує SIEM, UEBA, DPI-аналіз та поведінкове моделювання, дозволило скоротити середній час виявлення інцидентів та знизити кількість хибнопозитивних спрацювань. Результати свідчать про доцільність інтеграції

аналітичних інструментів із людським експертним контролем, що забезпечує високий рівень захисту навіть від складноструктурованих атак.

Практична значимість дипломної роботи полягає в тому, що її результати та матеріал можна використати для покращення функціонування корпоративних мереж. Отримані результати можуть слугувати основою для подальших досліджень та впровадження систем кіберзахисту у сфері державного управління, критичної інфраструктури та комерційного сектору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аулов І.Ф., Нємцев Е.М. Сучасні методи та засоби захисту інформації в корпоративних мережах. Наукові записки Українського науково-дослідного інституту зв'язку. 2022. №4(64). С. 56-73.

2. .Бурячок В.Л., Толюпа С.В., Аносов А.О. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. Київ: ДУТ, 2021. С. 357.

3. Бекренєв В.І. Використання технологій штучного інтелекту в системах кібербезпеки. Кібербезпека в Україні. 2023. №1. С. 44-52.

4. Вовк І.І., Кириленко А.М. Аналіз нормативної бази України щодо управління інцидентами кібербезпеки. 2022. №1. С. 102-109.

5. Гнатюк С.Н., Приймак С.А. Системний підхід до моніторингу інформаційних подій в інфраструктурі підприємства. 2023. №1. С. 19-27.

6. Грицюк Ю.І., Дудикевич В.Б. Безпека інформаційних технологій: підручник. Львів: Видавництво Львівської політехніки. 2022. С. 320.

7. Закон України “Про основні засади забезпечення кібербезпеки України”, стаття 9, пункт 3.

8. Іваніченко Є.В., Сабліна М.А., Кравчук К.В. ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ В КІБЕРБЕЗПЕЦІ. 2021. С. 1-10.

9. Кабанов А.С., Лось В.П. Проактивний моніторинг як ключовий елемент сучасних систем захисту інформації. Безпека інформації. 2022. Том 28.

10. Коваленко П.О. Побудова моделей UEBA для корпоративного середовища. Вісник НТУУ "КПІ". Серія: інформатика, управління та обчислювальна техніка. 2023. №1. С. 58-64.

11. Козачок В.А., Дудикевич В.Б. Методи аналізу мережевого трафіку для виявлення атак на корпоративні мережі. Вісник Національного університету "Львівська політехніка". 2022. №1. С. 76-89.

12. Колесников С.П., Гудзь А.М. Виявлення загроз в інформаційних системах на основі поведінкового аналізу. Інформаційні технології і засоби навчання. 2022. №3. С. 83-97.

13. Корольов В.Ю., Ходаківський В.М. Застосування глибокого навчання для виявлення аномалій у мережевому трафіку. Наукові записки Українського науково-дослідного інституту зв'язку, 2022. №3(63). С. 44-58.

14. Корченко О.Г., Терейковський І.А., Карпінський М.П. Сучасні системи виявлення атак: монографія. Київ: ЦУЛ. 2023. С. 298.

15. Кузнєцов М.Ю., Павленко Є.О., Логін Т.І. Методи підвищення інтерпретованості моделей машинного навчання для задач кібербезпеки. Інформаційна безпека держави, суспільства та особистості. 2023. №2. С. 115-128.

16. Кулешов А.О., Шелестов А.Ю. Візуалізація даних у системах моніторингу кібербезпеки. Захист інформації. 2023. Том 25, №2. С. 101-112.

17. Миніна О.О., Станкевич С.В. Методи виявлення атак у мережах передачі даних з використанням систем типу IDS. 2021. №2. С. 36-45.

18. Мотичак Л.В., Шестак Я.В., Балич Б.Я. Архітектура систем моніторингу кібербезпеки в реальному часі. Сучасний захист інформації. 2023. №4. С. 88-97.

19. Пилипчук О.П., Гуменюк С.І. Захист інформації в комп’ютерних системах: навчальний посібник. Київ: КНУБА. 2021. С. 210.

20. Рій Р.В, Плесканка Н.О, Кирик М.В. ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ МЕТОДУ ISOLATION FOREST ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ. URL: https://heraldts.khmnu.edu.ua/index.php/heraldts/article/download/1315/1607/5210

21. Сидоренко В.М. Системи виявлення та запобігання атак: класифікація та практичні аспекти реалізації. Наукові записки Університету інформаційних технологій та менеджменту. 2022. №2. С. 67-74.

22. Про основні засади забезпечення кібербезпеки України. Відомості Верховної Ради (ВВР). 2017. № 45. С. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

23. Хомутовський С.П. Автоматизація реагування на інциденти за допомогою систем SOAR. Захист інформації. 2023. №4. С. 22-29.

24. ПРОБЛЕМИ ЧИННОЇ ВІТЧИЗНЯНОЇ НОРМАТИВНО-ПРАВОВОЇ БАЗИ У СФЕРІ БОРОТЬБИ ІЗ КІБЕРЗЛОЧИННІСТЮ: ОСНОВНІ НАПРЯМИ РЕФОРМУВАННЯ. Аналітична записка URL: https://www.niss.gov.ua/doslidzhennya/nacionalna-bezpeka/problemi-chinnoi-vitchiznyanoi-normativno-pravovoi-bazi-u-sferi

25. Стандарт ISO/IEC 27035 URL: https://isocert.org.ua/iso-iec-27035/

26. Ahmad A., Maynard S., Park S. Information security strategies: towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing. 2023. Vol. 34. P. 297-315.

27. Alessandri G., Manta F. Automated Detection and Response to Cyber Attacks: The Evolution of Intrusion Prevention Systems. International Journal of Network Security. 2023. Vol. 25. No. 1. P. 102-115.

28. Argentieri G. Exploring Network Vulnerabilities: Techniques for Unauthorized Access and Exploiting Weaknesses. 2 About Vulnerabilities, 3 Background on Techniques for Exploiting Vulnerabilities. P. 3-9. URL: https://www.theseus.fi/handle/10024/878275

29. Davis R., Cheng L. Visual Analytics for Cybersecurity: Challenges and Opportunities. ACM Computing Surveys. 2024. Part. 57. No. 3 P. 1-34.

30. Hoffman L., Peterson K. Next-Generation Cybersecurity: Integrated Approaches to Threat Detection and Response. IEEE Security & Privacy. 2024. Part. 22, No. 1. P. 45-56.

31. Kim D., Solomon M. Fundamentals of Information Systems Security. 4th ed. Jones & Bartlett Learning. 2022. P. 560.

32. Miller D., Thompson K. Indicators of Compromise: Effectiveness and Limitations in Modern Cyber Defense. Journal of Cybersecurity. 2023. Vol. 9. No. 2. P. 1-17.

33. Mitropoulos D., Karakoidas V., Spinellis D. Incident Management for IT Systems. 2022. P. 270.

34. National Institute of Standards and Technology. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. Special Publication 800-83. Gaithersburg: NIST. 2023. P. 47.

35. National Institute of Standards and Technology. Guide to Intrusion Detection and Prevention Systems (IDPS). Special Publication 800-94. Gaithersburg: NIST. 2022. P. 59.

36. Northcutt S., Novak J. Network Intrusion Detection. 3rd ed. New Riders Publishing. 2021. P. 416.

37. S. Bhuyan et al. Network Anomaly Detection: Methods, Systems and Tools – A Survey. IEEE Communications Surveys & Tutorials. 2014. Vol. 16. No. 1.

38. Schneider B., Anderson C. The Role of Deception Techniques in Cybersecurity Research and Practice. Communications of the ACM. 2023. Part. 66, No. 7. P. 82-91.

39. Stallings W. Network Security Essentials: Applications and Standards. 7th ed. Pearson. 2022. P. 480.

40. Solodovnik, A., & Tatarinov, S. Use of Open-Source SIEM Solutions in SME Environments: Case Study on Wazuh. Information Security Journal. 2021. Vol. 30(4). P. 195-201.

41. Wazuh. Security information and event management *(SIEM)*. URL: https://documentation.wazuh.com

42. Zuech R., Khoshgoftaar T.M., Wald R. Intrusion detection and Big Heterogeneous Data: A Survey. 2022. Vol. 9. Art. 31.