МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ОПТИМІЗАЦІЯ ПРОЦЕСУ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРАТАКИ У СТРУКТУРАХ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ”

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

_____ Ігор ФОМІН
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач(ка) вищої освіти гр. УБД-42
Ігор ФОМІН
Ім’я, ПРІЗВИЩЕ

Керівник: Дмитро РАБЧУН
Д.т.н., старший викладач Ім’я, ПРІЗВИЩЕ

Рецензент: Володимир КОНДРАТ
К.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Фоміну Ігору Олеговичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Оптимізація процесу виявлення та реагування на кібератаки у структурах малих та середніх підприємств”,
керівник кваліфікаційної роботи РАБЧУН Дмитро, д.т.н., старший викладач,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “__“ березня 2024 р. №__.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби виявлення та реагування на кібератаки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати особливості процесів виявлення та реагування на кібератаки у структурах малих та середніх підприємств .
4.2. Дослідити основні характеристики технологій виявлення та реагування на кібератаки.
4.3. Вивчити інструменти та методи оптимізації процесів виявлення та реагування на кібератаки у структурах малих та середніх підприємств, розробити практичні рекомендації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	11.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз теоретичних основ інформаційної безпеки малих та середніх підприємств.	08.04.2024	
4.	Дослідження основних характеристик технологій формування обізнаності й навчання персоналу.	22.04.2024	
5.	Дослідження технологій виявлення та реагування на кібератаки	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувачка вищої освіти _____ Ігор ФОМІН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Дмитро РАБЧУН
(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 здобувачка Фомін І.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Оптимізація процесу виявлення та реагування на кібератаки у структурах малих та середніх підприємств "

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ФОМІН Ігор у кваліфікаційній роботі проаналізував особливості процесів виявлення та реагування на кібератаки у структурах малих та середніх підприємств, дослідив основні характеристики технологій виявлення та реагування на кібератаки, вивчив інструменти та методи оптимізації процесів виявлення та реагування на кібератаки у структурах малих та середніх підприємств, розробити практичні рекомендації.

ФОМІН Ігор 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 одній конференції.

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

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Фомін І.О. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ФОМІНА Ігор
на тему "Оптимізація процесу виявлення та реагування на кібератаки у структурах малих та середніх підприємств"

Актуальність. У світі, де держави, компанії є об'єктами кібератак, важливість забезпечення інформаційної безпеки є великою, як ніколи. Тому важливо формувати комплексний підходу, який включає технічні засоби для ефективного протистояння сучасним кіберзагрозам, зменшуючи ризики втрат даних та фінансових збитків. Аналіз підходів до виявлення та реагування на кібератаки можуть допомогти в протистоянні сучасним кіберзагрозам, зменшуючи ризики втрат даних та фінансових збитків.

З огляду на зазначене дослідження оптимізація процесів виявлення та реагування на кібератаки у структурах малих та середніх підприємств є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено особливості оптимізації процесів виявлення та реагування на кібератаки у структурах малих та середніх підприємств .
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Автор опрацював значну джерельну базу: близько 40 публікацій, в тому числі 35 англомовних.
4. За результатами дослідження запропоновано рекомендації щодо оптимізації процесів виявлення та реагування на кібератаки у структурах малих та середніх підприємств.

Недоліки.

Доцільно було б приділити більше уваги вивченню і класифікації програмних інструментів для оцінки ефективності процесів виявлення та реагування на кібератаки у структурах малих та середніх підприємств .

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

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

Рецензент: _____ Олександр КОНДРАТ
к.т.н., доцент *підпис* Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню процесі виявлення та реагування на кібератаки у структурах малих та середніх підприємств. Робота складається зі вступу, трьох розділів, що містять 18 рисунків, висновків і списку використаних джерел із 40 найменувань. Загальний обсяг роботи становить 64 аркушів, з яких 4 аркуші займають перелік умовних скорочень та список використаних джерел.

Метою роботи є розробка рекомендацій щодо впровадження систем виявлення та реагування на кібератаки в мережеву інфраструктуру малих та середніх підприємств.

Об'єктом дослідження є підходи до побудови системи захисту мережевої інфраструктури малих та середніх підприємств на основі системи виявлення та реагування на кібератаки.

Предмет дослідження – системи виявлення та реагування на кібератаки у структурах малих та середніх підприємств.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, порівняння, класифікації, експертної оцінки.

Як результат у роботі проаналізовано особливості процесів виявлення та реагування на кібератаки у структурах малих та середніх підприємств, досліджено основні характеристики технологій формування виявлення та реагування на кібератаки; вивчено інструменти та методи виявлення та реагування на кібератаки, розроблено практичні рекомендації для підвищення ефективності реагування на кібератаки.

Галузь застосування. Розроблені підходи можуть бути використані при побудові системи захисту мережевої інфраструктури малих та середніх підприємств на основі системи виявлення та реагування на кібератаки.

Ключові слова: УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, РЕАГУВАННЯ НА КІБЕРАТАКИ, ОПТИМІЗАЦІЯ ПРОЦЕСІВ.

ABSTRACT

The qualification work is devoted to the study of information security awareness and training technologies for personnel. The work consists of an introduction, three chapters containing 18 figures, conclusions and the list of references containing 40 items. The total volume of the work is 63 pages, of which 3 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to develop recommendations for the implementation of cyber attack detection and response systems in the network infrastructure of small and medium-sized enterprises.

The object the study is approaches to building a system for protecting the network infrastructure of small and medium-sized enterprises based on a system for detecting and responding to cyber attacks.

The subject of the study is systems for detecting and responding to cyberattacks in the structures of small and medium-sized enterprises.

Research methods. In order to solve the above-mentioned scientific task, the paper uses the methods of analysis, comparison, classification, expert assessment, and a systematic approach to the processes of detecting and responding to cyberattacks.

As a result, the paper analyses the peculiarities of the processes of detecting and responding to cyberattacks in the structures of small and medium-sized enterprises, examines the main characteristics of technologies for forming detection and response to cyberattacks; examines tools and methods for detecting and responding to cyberattacks, and develops practical recommendations for improving the effectiveness of response to cyberattacks.

Field of application. The developed approaches can be used to implement a system for protecting the network infrastructure of small and medium-sized enterprises based on a system for detecting and responding to cyberattacks.

Keywords: INFORMATION SECURITY MANAGEMENT, RESPONSE TO CYBERATTACKS, OPTIMIZATION OF PROCESSES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ПЗ	Програмне забезпечення
СУБД	Система управління базами даних
МСП	Малі та середні підприємства
СВВ	Система виявлення вторгнень
СЗВ	Система запобігання вторгненням
СНД	Спроб несанкціонованого доступу
СУІБ	Система управління інформаційною безпекою
ШІ	Штучний інтелект
SIEM	Інформація про безпеку та управління подіями
QRadar	Система *SIEM*, розроблена *IBM*
ME	Міжмережеві екрани
IT	Інформаційні технології
SPL	Мова обробки пошукових запитів
VPN	*Virtual Private Network* (Віртуальна приватна мережа)
SIM	*Security Information Management* (Управління інформацією про безпеку)
SEM	*Security Event Management* (Керування подіями безпеки)
CMDB	*Configuration Management Database* (База даних керування конфігураціями)
SOC	*Security operations center* (Оперативний центр безпеки)
СМПБ	Системи моніторингу подій безпеки)
ОС	Операційна система
UDP	*User Datagram Protocol* (Протокол користувальницьких датаграм)
TCP	*Transmission Control Protocol* (Протокол керування передачею)

ВСТУП

Актуальність теми. За останні роки кіберзлочинці стали більш активнішими та вдосконалили свої методи атак, що часто націлені на слабкі сторони інфраструктури. Це змушує підприємства поставати перед викликом постійних змін та вдосконалень своїх заходів кібербезпеки. І враховуючи, що малим та середнім підприємствам часто бракує ресурсів для повноцінного захисту, оптимізація процесів виявлення та реагування на кібератаки дозволить ефективніше використати наявні ресурси. Дослідження у цій області важливе для забезпечення безпеки підприємств та збереження їхньої конкурентоспроможності на ринку.

З огляду на зазначене дослідження технологій формування обізнаності й навчання персоналу з інформаційної безпеки є актуальним науковим завданням.

Мета роботи полягає у розробці рекомендацій щодо впровадження систем виявлення та реагування на кібератаки в мережеву інфраструктуру малих та середніх підприємств.

Об'єкт дослідження – підходи до побудови системи захисту мережевої інфраструктури малих та середніх підприємств на основі системи виявлення та реагування на кібератаки.

Предмет дослідження – системи виявлення та реагування на кібератаки у структурах малих та середніх підприємств.

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

1. Проаналізувати теоретичні основи інформаційної безпеки малих та середніх підприємств.

2. Проектування системи виявлення кібератак.

3. Проектування системи реагування на кібератаки.

4. Розробка та впровадження системи виявлення та реагування на кібератаки.

Методи дослідження. Для вирішення означеного вище наукового

завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до управління інформаційною безпекою.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу ефективніше використати наявні ресурси малих та середніх підприємств для виявлення та протидії кіберзагрозам.

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

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ

Тема інформаційної безпеки малих та середніх підприємств є важливою в сучасному світі, оскільки багато аспектів діяльності підприємств залежать від комп'ютеризації та мережевого зв'язку. МСП включають в себе різноманітні бізнеси, починаючи від магазинів і ресторанів до виробничих підприємств та IT-компаній.

Однак залежність від інформаційних технологій також створює ризики. Кіберзлочинці, конкуренти та інші зловмисники можуть використовувати цю залежність для здійснення кібератак, спрямованих на підрив діяльності МСП. Навіть короткочасне втручання в роботу таких підприємств може мати серйозні наслідки для їхньої діяльності, фінансового та репутаційного стану.

Для забезпечення інформаційної безпеки МСП необхідно вживати комплекс заходів. Це включає в себе захист мережевих з'єднань, регулярне оновлення програмного забезпечення, використання сучасних засобів шифрування даних, а також впровадження систем виявлення та реагування на кіберзагрози.

МСП часто мають обмежені ресурси, тому важливо використовувати доступні інструменти та послуги, що допоможуть захистити їх інформацію та діяльність.

Співпраця з іншими підприємствами та організаціями також є ключовою. МСП можуть обмінюватися досвідом та найкращими практиками в сфері інформаційної безпеки, а також отримувати підтримку від державних і міжнародних організацій. Та користуватись за можливості послугами приватних компаній для оптимізації кібербезпекових процесів

Інформаційна безпека МСП вимагає комплексного підходу, включаючи технічні та програмні заходи, співпрацю з іншими підприємствами та установами. Тільки за умови такого підходу можна забезпечити надійний захист малих та середніх підприємств від кіберзагроз.

1.1 Аналіз загроз кібербезпеці для малих та середніх підприємств

Не можна недооцінювати роль інформаційно-комунікаційних технологій у сучасному бізнесі. Незважаючи на те, що такі технологічні досягнення надають численні переваги та можливості, вони, як відомо, також створюють для організацій нові завдання, як кібератаки. Це особливо важливо для МСП, які вважаються найменш зрілими та дуже вразливими до ризиків кібербезпеки.

В останнє десятиліття хвилі цифрової трансформації примусили МСП прийняти та оснастити свої бізнес-моделі технологіями, що постійно розвиваються. Ця закономірність прослідковуються від чи то онлайн-магазини або система керування ланцюгами постачання фірм. Технологічний прогрес створив нові та захоплюючі можливості для бізнесу, а також призвів до до нових викликів, які змінили організаційний дизайн, здатність керувати даними та додав нові джерела ризиків.

Породжені хвилею цифрової трансформації нові перешкоди, як такі як інформаційна безпека та кіберризики, призвели до значних фінансових та нефінансових втрат. Між тим вважається, що МСП стикаються з тими ж проблемами кібербезпеки, що і їхні великі колеги, однак обмеженість ресурсів та можливостей робить їх вразливими до кіберзагроз. Це означає, що управління кібер-ризиками та підготовка до них стають ключовими компетенціями не лише для виживання, але й для подальшого зростання малих фірм.

У контексті зростаючої важливості інформації, особливо враховуючи підвищену залежність від Інтернету в епоху цифрових технологій, дані стали критично важливим активом для будь-якої організації. Оскільки вимоги щодо доступу до інформації з боку різних зацікавлених сторін зростають, це викликає значні проблеми з безпекою [1]. Значна залежність від цифрових платформ у різних галузях підкреслює необхідність надійних заходів безпеки для захисту цього цінного ресурсу. Завд’яки чому підвищилась вразливість критично важливих даних до різних загроз кібербезпеці.

Ризики загрожують конфіденційності, цілісності та доступності інформації. Це розпочинає перегони між законними організаціями, так і зловмисниками що намагаються отримати доступ до цих даних [1]. Кіберзлочинці, використовуючи все більш витончені методи, посилюють загрози безпеці. Ця ескалація особливо помітна в секторі малого бізнесу, де фінансові обмеження часто обмежують виділення значних ресурсів на превентивні заходи безпеки, роблячи ці підприємства особливо вразливими до атак.

Тепер проаналізуємо чому кіберзлочинці зацікавленні в атаці на МСП. На глобальному рівні МСП відповідають за понад 90 відсотків світової бізнес-економіки [1]. Аналізуючи загрози кібербезпеки для малих та середніх підприємств, важливо розуміти, що ці організації часто стикаються зі специфічними викликами та вразливостями через свій розмір, ресурси та стратегії кібербезпеки.

Згідно статистиці 2023 року, 66% МСП повідомили, що зазнали кібератаки протягом попередніх 12 місяців [2]. Ця статистика викликає занепокоєння не лише у малих та середніх підприємств, але й у постачальників та клієнтів, які ведуть з ними бізнес.

Інше дослідження показує загрози інформаційній безпеці, з якими зіткнулися підприємства: 45% підприємств зазнали витоку інформації завдяки фішингу, 62% неавторизованого доступу, 83%, 24% атаки різноманітних шкідливих програм [3]. Крім того, інформаційні загрози у більшості випадків можуть бути спричинені необізнаністю працівників, опором змінам, недобросовісною поведінкою, недостатнім для займаної посади рівнем обізнаності та доступом до невідомих та не перевірених веб-сайтів або карт пам'яті з зовнішніми дисками.

Результати показують, що всі відібрані підприємства стали жертвами інформаційних загроз. Вплив інформаційних загроз послаблює конфіденційність, цілісність, доступність і авторизований доступ бізнес-інформації. До інформаційних загроз також відносяться нав’язливі та бентежачі

атаки, цілю котрих є відточення навичок кіберзлочинцями, та які націлені на сектору малого бізнесу. І незважаючи на те, що деякі компанії виділили ресурси на розробку стратегії пом'якшення наслідків від подібних атак, вони можуть наштовхнутись на відмову в обслуговуванні обладнання або ПЗ, тимчасовою недоступністю даних, незареєстрованим система безпеки несанкціонованим доступом, які призведуть до порушення конфіденційності, приватності та цілісності, що в кінцевому підсумку теж приведе до витоку даних. Ці порушення інформаційної безпеки спричинені інсайдерами та аутсайдерами [3].

Загрози інсайдерської інформації часто можуть спричинятись необізнаністю працівників, невірно або невчасно прийняттями рішеннями, браком кваліфікаційних навичок, неефективними або застарілими впровадженими стратегіями безпеки, нестачею персоналу, поганими настановами з безпеки та прогалинами в технологічних знаннях [3].

До загроз аутсайдерської діяльності зазвичай відносяться несанкціоновані дії осіб які не мають легітимного доступу до організаційних систем. Цього можна досягти за допомогою різних засобів, починаючи від таких методів як злом, фішинг, зловмисне програмне забезпечення закінчуючи співробітниками, підрядниками або будь-ким, хто має законний доступ до систем організації, але використовує цей доступ у зловмисних цілях.

Також до загроз для кіберберзпеки підприємств відносяться загрози конфіденційності інформації. Під цими загрозами прийнято приймати реальні або потенційні імовірні дії по відношенню до інформаційних ресурсів, що призводять до неправомірного здобування охоронюваними відомостями [3]. Такими діями є:

– перегляд конференційною інформацією різноманітними шляхами і способами без порушення її цілісності;

– зміна інформації в злочинних цілях як часткова або значна зміна складу і змісті відомостей;

– знищення інформації як акт вандалізму з метою прямого нанесення матеріального збитку.

Відповідно це призводить до порушення її:

– конфіденційності;

– цілісності;

– доступності.

Тобто інформацію, як один із основних активів бізнесу, слід завжди захищати та охороняти від поширених, руйнівних, проникаючих загроз. Інформаційна безпека, яку ще іноді називають *InfoSec*, захищає інформацію від несанкціонованого доступу, використання, розголошення, зміни, запису, перевірки або запису. А отже, інформаційна безпека повинна ставати пріоритетом у всіх установах. Практика інформаційної безпеки запобігає несанкціонованому доступу до інформації, несанкціонованій зміні та видаленню даних. Мережа та комп'ютер є основними інструментами, які використовуються для розгортання витоків даних, як правило, у вигляді вірусів, спаму, фішингу та крадіжки особистих даних. Ці витоки даних порушують конфіденційність, цілісність і доступність бізнес-інформації, що теж відноситься до фундаментальних принципів інформаційної безпеки (Рис.1.1)[3].

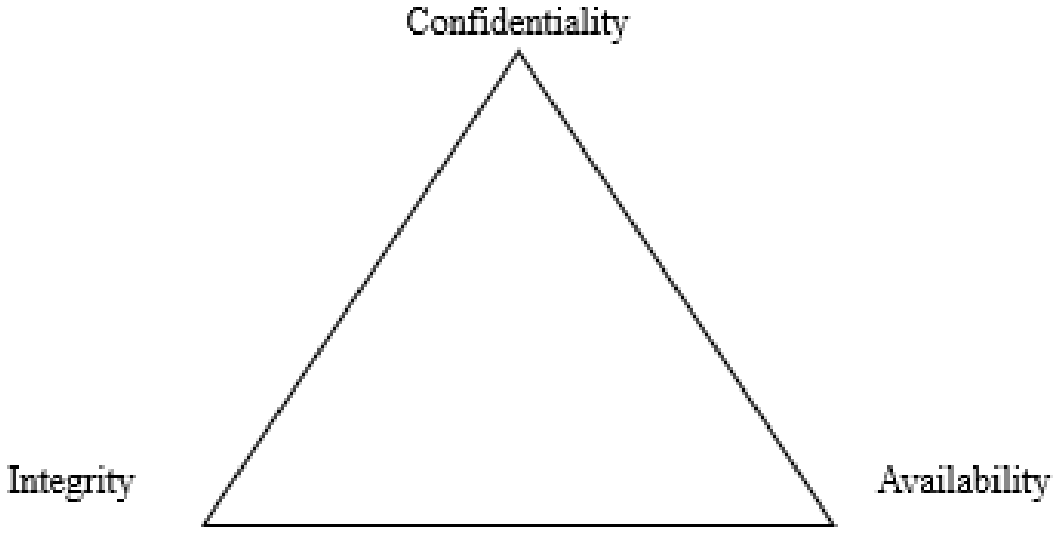

Рис. 1.1. Принципи безпеки тріади *CIA*

На рисунку 1.2 зображена мета інформаційної безпеки.

Рис. 1.2. Загроза інформації

До типів загроз кібербезпеці для МСП відносяться:

- фішинг;
- програми-вимагачі;
- шкідливі ПЗ;
- експлойти нульового дня;
- інсайдерські загрози;
- соціальна інженерія;
- *ddos*-атаки;
- *sql*-ін’єкції.

Дослідження компанії *Verizon* у своєму "Звіті про розслідування витоків даних за 2023 рік" підкреслює, що серед наведених типів загроз найбільш поширеними залишається фішинг. Він є значною загрозою, оскільки значний відсоток витоків відбувається саме через такі атаки [4].

До фішингу відносяться спроби викрасти конфіденційну інформацію за допомогою оманливих електронних листів або повідомлень, що видають себе за листи від надійних організацій. МСП особливо вразливі, оскільки їхні працівники можуть бути недостатньо навчені розпізнавати такі шахрайства.

На рисунку 1.3 зображена структура типів загроз кібербезпеці для МСП.

Рис. 1.3. Структура типів загроз кібербезпеці для МСП

1.2 Огляд існуючих методів та технологій виявлення кібератак

На думку фахівців загрози кібербезпеці для МСП стали більш прогресивними, націленими на вразливі місця, тому виявлення таких загроз стає пріоритетним завданням. Існуючі методи та технології для виявлення кібератак використовують інтегрований підхід до безпеки. Такий підхід включає не тільки ізольовані захисні бар'єри на периферії мережі, але й цілий комплект компонентів, таких як сканери вразливостей, системи аутентифікації та авторизації, інструменти для створення віртуальних приватних мереж тощо. Одним з ключових елементів такої комплексної системи захисту інформації — засоби виявлення вторгнень. Функція засобів виявлення вторгнень полягає в аналізі підозрілих дій, що відбуваються у захищеній інформаційній системі.

Різноманіття інструментів та стратегій для ідентифікації зловмисних дій допомагає виявити атаку до того, як вона завдасть значної шкоди. Досліджено, що ключовими серед цих методів є:

1. Системи виявлення вторгнень відноситься до програмних або апаратних систем завданням яких є відстеження мережевого трафіку на наявність підозрілої активності та відомих загроз, повідомляючи адміністраторів про можливі порушення. Наділі для стислості викладу систему моніторингу подій називатимем СВВ. Виявлення вторгнень відноситься до процесу моніторингу подій, що відбуваються в мережі або комп’ютерній системі з подальшим їх аналізом. При виявлені атаки СВВ превентивних заходів зазвичай не вживає. До СВВ відносяться програмні та апаратні

пристрої, які дозволяють автоматизувати процес моніторингу та аналізу подій, що відбуваються в мережі або системі, з метою виявлення вторгнень. СВВ складаються з трьох функціональних компонентів: інформаційних джерел, аналізу та відповіді. СВВ отримує інформацію про подію з одного або більше джерел інформації, виконування визначається конфігурацією під час аналізу даних події і потім створюються особливі відповіді – від найпростіших звітів до активного втручання при визначенні проникнень. Розміщення СВВ може бути на основі мережі або на основі хосту, кожна з яких пропонує унікальні переваги для малих і середніх підприємств з точки зору масштабу та можливостей виявлення [5].

2. Управління інформацією про безпеку та подіями: система в якій поєднуються інструменти керування подіями безпеки, що дозволяє аналізувати дані журналів і подій у режимі реального часу, щоб забезпечити моніторинг загроз, кореляцію подій і реагування на інциденти, з керуванням інформацією про безпеку, яке збирає, аналізує дані журналів і звітує про них [6]. Завдяки чому забезпечується цілісне уявлення про безпеку організації. А за допомогою збору та аналізу даних журналу з різних джерел, полегшує виявлення складних кіберзагроз використовуючи правила кореляції та розпізнавання шаблонів.

3. Виявлення та реагування на кінцеві точки: система, що постійно відстежує і збирає дані для виявлення моделей загроз. Це обумовлено тим, щоб мати змогу в реальному часі відстежувати дії користувачів і попереджати, якщо дії почнуть відхилятися від встановлених норм. Системи включають в своєму функціоналі можливість розпізнавати та розуміти складні патерни поведінки і тим самим розрізняти доброякісні аномалії від справжніх загроз. До особливості системи є здатність автоматичного реагування, що дозволяє нівелювати ефект несподіванки та звести шкоду до мінімуму. Коли загрозу перевірено, системи автоматичного реагування можуть виконувати заздалегідь визначені дії для стримування та нейтралізації ризику, часто без необхідності втручання людини. До вже наведеного функціоналу наведемо, що в системі присутній функціонал виявлення зловмисного програмного забезпечення та

інших специфічних для кінцевих точок загроз, які входять до типових атак на МСП [7].

4. Рішення для виявлення фішингу: спеціалізовані рішення, які використовують машинне навчання та штучний інтелект для аналізу вхідних повідомлень на наявність ознак спроб фішингу [8]. Шляхом чого дозволяють значно підвищити рівень безпеки працівників за рахунок забезпечення безпеки електронної пошти малого та середнього бізнесу шляхом автоматичної ідентифікації та розміщення підозрілих електронних листів на карантин, таким чином зменшуючи залежність від розсудливості та навченості користувачів.

До недоліків систем виявлення вторгнення відносяться:

– відсутність тестів продуктивності і покриття мережі;

– відсутня універсальна методологія проектування;

– недостатня мобільність в контрольованому просторі;

– обмежена гнучкість (включає універсальність і динамічне налаштування);

– обмежена можливість оновлення методів виявлення;

– труднощі з підтримкою наборів правил функціонування.

Коректність інформації пропорційно впливає та визначає точність заходів. Тому за допомогою цілого ряду різноманітніших джерел інформації, які дозволяють проаналізувати та ідентифікувати невідповідності в поведінці, є одним із способів забезпечити необхідну точність виявлення. Для покращення ефективності в виявленні є доцільним використання баз правил, бібліотек функцій, бібліотек атак. Це також дозволяє підвищити ефективність реагування на інциденти.

Системи виявлення вторгнень, поділяються на декілька видів, а саме:

- Прикладна система виявлення вторгнень;
- Мережева система виявлення вторгнень;
- Система виявлення вторгнень на основі хоста або вузлова.

Прикладні СВВ аналізують події, які надійшли програмне забезпечення

програми. Загальними джерелами інформації звідки надходить інформація є: лог файли транзакцій додатків. Завдяки здатності взаємодіяти з додатком, з з конкретним доменом або застосовувати інформацію, специфічну для докладання, надає змогу прикладній СВВ визначати підозрілу поведінку авторизованих користувачів, що перевищує їх права доступу. Такі проблеми можуть проявитись лише при взаємодії користувача з додатком [9].

Мережева СВВ відноситься до програмного процесу, котрий працює на спеціально виділеній системі, і відповідає за перемикання мережевої карти в системі в режим роботи, при якому мережевий адаптер пропускає весь мережевий трафік в програмне забезпечення. Використовуючи набір правил і ознак атак для розпізнавання того, чи представляє цей трафік якийсь інтерес відбувається аналіз трафіку. Після чого генерується відповідна подія. При відсутності ознак атаки в СВВ, система не відмічає цю атаку. Дані системи дозволяють вибирати певне джерело трафіку за адресою джерела, кінцевій адресі, порту джерела або кінцевого порту. Це надає можливість відстежувати трафік, що підпадає під ознаки атаки.

Вузлові СВВ, приставляють систему датчиків котрі завантажуються на різні сервера організації і керуються центральним диспетчером. Датчики відстежують різні типи подій і виконують певні дії на сервері або надсилають повідомлення. За допомогою датчиків також відстежуються події, що пов’язані з сервером, на якому вони завантажені. Сенсор вузлових СВВ дозволяє визначити, чи була атака успішною, якщо атака відбулась на тій же платформі, що і датчик. Для роботи датчика на сервері потребується достатня кількість загального процесорного часу. Зазвичай споживання процесорного часу доходить до 15% [9]. Тому з’являється необхідність в придбанні більш продуктивнішої системи, щоб присутність датчика негативно не позначилася на продуктивності використовуваної системи.

В даній системі присутні п’ять головних типів датчиків:

– аналізатор журналів;

– датчик ознак;

– аналізатор поведінки додатків;

– контролери цілісності файлів;

– аналізатор системних викликів.

Проаналізуємо функціонал цих датчиків:

1. Аналізатори журналів це процес, виконуються на сервері та відповідає за відстеження файлів журналів в системі. Під час виконання процес перевіряє відповідність записів у журналі і в відповідності до встановлених критеріїв ВСВВ, виконує встановлену дію. Вибір журналу запису, що підпадатиме під аналіз може визначити адміністратор системи. Аналізатори журналів не запобігають атаці на систему, а реагують на подію вже після того, як воно сталося [10]. Аналізатор журналів підходить для використання відстеження активності і переміщення запису про активність персоналу в область, недосяжну для адміністратора або користувача.

2. Датчик ознак відноситься до процесу, що виконує, порівняння вхідного трафіку або записів в журналах з наборами певних характеристик що відповідають подіям безпеки. Здатність аналізувати вхідний трафік відрізняє ці датчики від аналізаторів журналів [10]. Датчик ознак ВСВВ корисний для моніторингу авторизованих користувачів у межах інформаційних систем.

3. Аналізатори системних викликів є процесом, що здійснює аналіз викликів між додатками і операційною системою для ідентифікації подій, пов’язаних з безпекою. Сенсори цього типу створюють програмний міст між операційною системою та додатками. Коли додаток виконує дії, його системний виклик перевіряється на відповідність з базою даних характеристик, які включають приклади атакуючих дій або інших дій, що мають інтерес для адміністраторів системи виявлення вторгнень. Аналізатори системних викликів відрізняються від інших згаданих датчиків тим, що вони можуть запобігати певним діям. Неправильна конфігурація або налаштування датчиків може призводити до помилок у додатках або навіть до їхньої непрацездатності [10].

4. Аналізатори поведінки додатків Використовуються як програмний інтерфейс між додатками та операційною системою, ці інструменти

перевіряють, чи має додаток дозвіл на виконання конкретної дії, замість того, щоб перевіряти відповідність виклику ознакам атаки. Під час налаштування таких сенсорів важливо скласти список дій, які кожен додаток має право виконувати. Виробники цього типу сенсорів зазвичай надають стандартні шаблони для поширених додатків [10].

5. Контролери цілісності файлів відповідають за моніторинг змін в файлах, використовуючи криптографічну контрольну суму або цифровий підпис файлу (шифрування). Якщо хоча б незначну частину початкового файлу змінено (це може стосуватися атрибутів файлу, таких як час і дата створення), то кінцевий цифровий підпис файлу зазнає змін. Метою цього алгоритму є мінімізація можливості внесення змін у файл без зміни існуючого підпису. Під час первинної конфігурації датчика кожен файл обробляється для створення початкового підпису. Отримане значення служить доповненням до підпису і, за потреби, порівнюється з оригіналом. Невідповідність свідчить про те, що файл було змінено. Контролер цілісності файлів не виявляє саму атаку, але вказує на результати здійсненої атаки.

1.3 Сучасні методи та технології реагування на кібератаки

У сучасному бізнес-середовищі, де кіберзагрози та інші небезпеки еволюціонують із кожним днем, належне реагування стає не просто важливим елементом, а абсолютною необхідністю для забезпечення безпеки та стабільності діяльності будь-якої компанії [11]. Відсутність або неналежне реалізування реагування на інциденти може призвести до значних фінансових втрат, втрати довіри з боку клієнтів та партнерів, а також до серйозних юридичних наслідків.

Розробка плану реагування на інциденти дозволяє команді з кібербезпеки ефективно реагувати та гарантувати, що нічого не проскочить. План реагування повинний містити, наступні ролі та обов’язки:

1. Хто: Необхідно розробити список осіб, до яких слід звертатися у випадку інциденту. Вкрай важливо знати, хто прийматиме рішення про початок

процедур відновлення і хто буде основною контактною особою з відповідними правоохоронними органами [12].

2. Що: Необхідно, мати розроблений план дій, що буде відбуватись з даними у випадку інциденту [12]. Дії можуть містити вимкнення або блокування комп'ютерних систем, переміщення інформації на резервне сховище та/або фізичне видалення важливих документів і конфіденційних матеріалів. Дії підбираються відповідно до наявного устаткування.

3. Коли: Визначте, при яких типах дій загроз, необхідно сповіщати вище керівництво, аварійний персонал, фахівців з кібербезпеки, юридичну консультацію, постачальників послуг або страхових компаній. Обов'язково вкажіть усю необхідну контактну інформацію [12].

4. Тип: план реагування повинен чітко визначати типи дій, які становлять інцидент інформаційної безпеки. План повинен містити інциденти, як непрацездатність вашого веб-сайту протягом більш ніж визначеного періоду часу або докази крадіжки інформації [12]. План адаптується під вимоги компанії, тому необхідно час від часу його оновлювати, для актуальності дій, для реагування на інциденти.

Автоматизація робочих процесів дозволить команді під час реагування не витрачати дорогоцінний час на дрібні процеси. Наприклад створення каналу ситуаційної кімнати в *Zoom* наповнення його потрібними людьми, клонування контрольного списку завдань дозволить ефективніше використати наявні часові ресурси.

Якщо план реагування не реалізований належним чином бізнес стає вразливим до різних загроз. В такому випадку необхідно мати план безперервності бізнесу, що включатиме план дій на випадок катастрофічних збоїв і порушень.. Такий план має включати встановлення резервного каналу для вашого зв’язку в системі, незалежної від вашої основної хмарної інфраструктури, щоб гарантувати, що служби першої допомоги ніколи не залишаться на зв’язку, незалежно від того, наскільки поширеним може бути інцидент [13]. Крім того планування менш катастрофічних, але все ж значних за

небезпекою відхилень від плану реагування на інциденти допомагає команді більш плавно виконувати свої дії. Наприклад, переконавшись, що кожне завдання має не лише призначеного власника, а й призначеного резервного власника, буде не допущено, щоб дії з реагування були збиті з колії через те, що відповідальні особи були у відпустці, захворіли чи іншим чином були недоступні.

Платформи для співпраці з реагування на інциденти дозволяють зберігати всі необхідні інструменти в одному місці. Що дозволяє отримати легкий доступ до них для команди з реагування, що гарантує, що кожен зможе швидко знайти те, що буде необхідно для виконання поставлених завдан. Також до функціоналу відноситься можливість команди з реагування та іншим підрозділам організації мати місце де вони повинні будуть обмінюватися інформацією в рамках робочих процесів реагування на інциденти. Докази, документація процесу та відстеження виправлень є критично важливими частинами спільної роботи з реагування на інциденти [13].

Належний план та комплекси програмного забезпечення, дозволяють зменшити вразливість до кіберзагроз. Використання МСП хмарних сховищ, які слугуватимуть безпечною системою резервного копіювання, оскільки хмарне сховище має високий рівень безпеки, що підвищить безпеку та безпеку інформації. Ідея полягає в тому, щоб створювати резервні копії даних відповідно до потреб кожного бізнесу [13]. Для деяких малих бізнесів можливо буде вистачати і безкоштовних хмарних сховищ. Компанії також повинні завжди мати антивірусні та антишпигунські програми з актуальними базами загроз. Це дозволить бізнес-пристроям, що підключені до мережі отримувати перевірені оновлення з надійних джерел, завдяки пристроям з антивірусним і антишпигунським програмним забезпеченням котрі автоматично запускатимуть оновлення для виявлення відхилень у бізнес-мережі та системі. Крім того, якщо фукнціонал пристрою дозволяє для підвищення безпеки, проводити шифрування даних на пристроях з подальшим доступ до них за допомогою токенів або інших криптографічних пристроїв.

Крім того, інвестування в комплекси програмного забезпечення для моніторингу, виявлення та блокування потенційних кіберзагроз є критично важливим для забезпечення цілісності та безпеки інформаційних активів компанії. Сучасні технології, такі як штучний інтелект та машинне навчання, можуть значно підвищити ефективність систем захисту, дозволяючи їм адаптуватися до нових загроз та забезпечувати проактивний захист. Інтеграція алгоритмів штучного інтелекту та машинного навчання в антивірусні програми значно підвищила їхню ефективність у виявленні, запобіганні та реагування зараженням шкідливим програмним забезпеченням. Аналізуючи великі обсяги з різноманітних джерел даних, виявляючи закономірності та потенційні загрози, антивірусне програмне забезпечення на основі ШІ та ML може забезпечити більш точний і своєчасний захист від широкого спектру онлайн-загроз.

Використання алгоритмів ШІ та ML в програмному забезпеченні дозволить підвищити ефективність виявлення та реагування. Основну інформацію про методи, що використовують *AI*/*ML* методи в своїй роботі, переваги та виклики, пов'язані з цими технологіями наведено в табл. 1.1 [14].

Таблиця 1.1

Переваги та виклики застосування методів штучного інтелекту та машинного навчання

AI/*ML* Методи	Переваги	Виклики
Алгоритми машинного навчання	Має можливість аналізувати величезні обсяги даних для розпізнавання та виявлення закономірностей що дозволяє прогнозувати потенційні загрози.	Потребує великої кількості даних для ефективного навчання моделі.
Алгоритми глибокого навчання	Може виявляти раніше невідомі загрози та адаптуватися до мінливих моделей атак	Вимагає актуальну базу загроз та значних обчислювальних ресурсів для ефективного навчання та роботи моделі.
Поведінкова технологія виявлення	Може відстежувати активність системи в режимі реального часу для виявлення підозрілої поведінки.	Під час роботи може генерувати хибно позитивні або негативні спрацювання, що призводить до непотрібних сповіщень.

Продовження таблиці 1.1.

AI/*ML* Методи	Переваги	Виклики
Поведінкова технологія виявлення	Може відстежувати активність системи в режимі реального часу для виявлення підозрілої поведінки.	Під час роботи може генерувати хибно позитивні або негативні спрацювання, що призводить до непотрібних сповіщень або пропущених загроз.
Прогнозне моделювання загроз	Може аналізувати великі обсяги даних для виявлення нових загроз і потенційних векторів атак.	Потребує точних вхідних даних та постійного оновлення, щоб залишатися ефективною.
Виявлення атак нульового дня	Може виявляти та блокувати раніше невідомі загрози	Може бути менш ефективним проти складних або цілеспрямованих атак
Машинне навчання з персоналізованою моделлю	Дозволяє впровадити та забезпечити індивідуальний захист на основі поведінки та вподобань користувача.	Потребує значної кількості обчислювальної потужності та ємності для зберігання, обробки та навчання
Моніторинг та аналіз у реальному часі	Може виявляти та реагувати на загрози в міру їх виникнення	Потребує значної кількісті ресурсів і може генерувати велику кількість сповіщень

Згідно табл. 1.1 наведені методи, дозволяють впровадити застосування ШІ та *ML* у сферу кібербезпеки. Що матиме потенціал для революції в цій галузі, але водночас створює низку викликів і перешкод на шляху до впровадження. Однією з найпоширеніших проблем є недостатнє розуміння технології, про що повідомили 36,9% опитаних організацій [14]. Таке нерозуміння може заважати організаціям ефективно оцінювати та впроваджувати рішення у сфері ШІ та *ML*. Це також перешкоджає їхній здатності ефективно керувати цими системами та контролювати їх.

До проблеми, що не дозволяє розпочати масове впровадження також варто віднести, те що для впровадження штучного інтелекту та машинного навчання в системи реагування потрібен ряд технічних навичок, зокрема наука про дані, машинне навчання та досвід у сфері кібербезпеки. Багатьом МСП може бути важко знайти й утримати персонал із такими навичками, особливо на конкурентному ринку праці. Іншим викликом та перешкодою є те, що для їх впровадження та підтримуванню роботи існує потреба в спеціалізованому апаратному забезпеченні та інфраструктурі. Існують також занепокоєння щодо

конфіденційності та безпеки даних під час навчання моделей і під час їх роботи, а також потенційну упередженість і помилки що на даний момент виникають в алгоритмах *AI* та *ML* [14].

Використання правильного набору даних важливим для ML, щоб підвищити його точність і скоротити час обробки. Нові набори даних, такі як *New Selected Learning-Knowledge Discovery in Databases Dataset*, пропонують набагато більш вражаючий рівень зібраних великих даних, які впливають на результати цих аномальних виявлень. Для ефективно обробляти та використовувати ці дані дозволяє алгоритм *Condensed Nearest Neighbors*. *CNN* використовує методи класифікації та регресії в методі керованого навчання для аналізу розподілу зразків. Використання *CNN* дозволяє зменшити споживання системних ресурсів, а також скоротити час обробки, зберігаючи при цьому хороші результати виявлення.

У неконтрольованому підході використовуваний набір даних не містить жодної інформації про клас. Він ґрунтується на моделі припущення та про те, що профіль користувача зловмисника не може змінитися за короткий час, а зловмисна діяльність викликає аномальні зміни в мережі. У цьому неконтрольованому стані алгоритм, який називається операційною логікою, використовується для створення цих передбачуваних класів зловмисників і відхилень за допомогою веб-перегляду та трафіку електронної пошти. Ці класи можуть мати або величезну кількість подій, або надзвичайно малу кількість подій. Перевагою тут є здатність виявляти атаки нульового дня. Недоліком є те, що зловмисник може виробляти інформацію про мережевий трафік, достатню для того, щоб обійти системи *IDPS*.

Важливу роль відіграє і навчання персоналу: регулярні тренінги та інформування співробітників про поточні загрози та методи їх запобігання можуть значно підвищити ефективність реагування на кібератаки. Освічені співробітники теж стають додатковим бар'єром на шляху кіберзлочинців.

Висновки до розділу 1

В цьому розділі було розглянуто фундаментальні знання, необхідні для розуміння складного ландшафту загроз кібербезпеці, з якими стикаються малі та середні підприємства (МСП). Це підкреслює критичний характер кібербезпеки в цифрову еру, де частота, витонченість і вплив кібератак продовжують зростати. У цьому розділі досліджено різні загрози кібербезпеці, зокрема фішинг, зловмисне програмне забезпечення та програми-вимагачі, а також те, як вони конкретно впливають на МСП, які часто менш підготовлені через обмеження ресурсів.

Досліджено, що незважаючи на обмежені ресурси, МСП є привабливими цілями для кіберзлочинців через їхні часто слабкіші протоколи безпеки та цінні дані, які вони зберігають. Це робить обов'язковим для малих і середніх підприємств прийняти проактивний підхід до кібербезпеки, залучаючи як технологічні рішення, так і організаційні стратегії. Необхідність використання комплексних систем виявлення та реагування, таких як системи безпеки інформації та управління подіями (*SIEM*), була детально розглянута, щоб продемонструвати, як вони можуть служити надійною опорою в інфраструктурі кібербезпеки малого та середнього бізнесу.

Встановлено, що отримані на основі аналізу дані, дозволять коректною та якісно спроектувати і реалізувати системи реагування та виявлення кібератa

Визначено, що цей розділ заклав основу для розуміння ролі, яку обізнаність і навчання відіграють у зміцненні кібербезпеки МСП. По мірі переходу до наступних розділів фокус буде зміщений у бік детального аналізу та оптимізації стратегій виявлення та реагування, які можна адаптувати до конкретних потреб і обмежень МСП.

Розділ 2 ПРОЕКТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ КІБЕРАТАК

В умовах зростаючих кіберзагроз система виявлення кібератак повинна забезпечувати захист інформаційних ресурсів від несанкціонованого доступу, втрат і модифікацій даних. Проектування та впровадження в мережеву інфраструктуру підприємства системи виявлення кібератак, яка здатна забезпечити своєчасне виявлення та реагування на загрози дозволить підвищити захищеність цифрових активів підприємств.

Для забезпечення ефективного виявлення кібератак необхідно вживати комплекс заходів. Це включає в себе використання спеціалізованих програмних та апаратних засобів для моніторингу мережевих з'єднань, аналізу трафіку, виявлення аномалій та підозрілої активності. Регулярне оновлення програмного забезпечення, використання сучасних засобів шифрування даних, а також впровадження систем виявлення та реагування на кіберзагрози є ключовими елементами проектування такої системи.

Для ефективного виявлення кібератак необхідно визначити основні вимоги до системи. Та проаналізувати підходи до виявлення кібератак, які можна застосувати в системах виявлення для МСП.

Система виявлення кібератак також повинна бути інтегрована з іншими компонентами кібербезпеки організації, забезпечуючи комплексний підхід до захисту інформаційних ресурсів.

Обмін інформацією про нові загрози та спільні заходи щодо їхнього виявлення та нейтралізації можуть значно підвищити ефективність систем виявлення кібератак.

Проектування системи виявлення кібератак вимагає персоналізованого підходу. Тільки за умови такого підходу можна забезпечити надійний захист інформаційних ресурсів від кіберзагроз.

2.1 Визначення вимог до системи виявлення кібератак для малих та середніх підприємств

Системи виявлення атак для малих та середніх підприємств – це програмні або апаратно-програмні рішення, які зазвичай автоматизують процес контролю подій, що протікають в інформаційній системі або мережі, а також мають функціонал до самостійного аналізу цих подій в пошуках ознак проблем безпеки. З доступністю технологій та навчальних посібників кількість різних типів і способів несанкціонованих проникнень у чужі мережі організації за останні роки збільшилася, системи виявлення атак (СВА) стали необхідним компонентом інфраструктури безпеки більшості організацій [15].

Вимоги до системи виявлення кібератак, можна узагальнити наступним чином:

– Точність: СВА повинна мати достатню згідно вимог підприємства точність виявлення кібератак;

– Швидкість: швидке виявлення кібератак дозволить мінімізувати потенційну шкоду, яку вони можуть завдати;

– Масштабованість: дозволить по мірі розростання мережевої інфраструктури підприємства, забезпечувати вказаний у вимогах рівень безпеки без внесення суттєвих змін в системі;

– Інтегрованість з іншими системами безпеки: дозволяє підвищити ефективність виявлення кібератак за рахунок інтеграції з функціоналом інших систем;

– Простота використання: є запорукою швидкої та ефективної взаємодії працівників з системою та її впровадження в безпекову інфраструктуру підприємства.

Виявлення та захист від великої кількості складних мережевих атак що спрямовуються на МСП є нагальною проблемою, яка потребує вирішення. Системи виявлення вторгнень (*IDS*), є досить поширеним рішенням для виявлення кібератак. У системах *IDS* використовуються методи, засновані на

сигнатурах і статистиці. Однак сигнатурні методи не можуть виявляти нові типи/варіанти атак, а ретельне попереднє визначення шаблонів такої великої кількості існуючих атак є складним завданням навіть для експертів, що суттєво впливає на ефективність виявлення *IDS*. Між тим, *IDS*, що базуються на статистичній інформації, завжди припускають, що нормальні або аномальні комунікації підпорядковуються певному розподілу, але очевидно, що це не так, і визначити параметри передбачуваного розподілу нелегко.

Враховуючи, що сучасні комп'ютерні продукти виявлення потребують дорого вартісного технічного оснащення, використання технології хмарних обчислень має величезний потенціал.

Обчислювальні хмари складаються з тисяч серверів, розміщених в дата-центрах, що забезпечують роботу десятків тисяч додатків, які одночасно використовують мільйони користувачів. Необхідною умовою для ефективного керування такою великою інфраструктурою є високий рівень автоматизації.

Для забезпечення різноманітних за вимогами видів користувачів – хмарним операторам, сервіс-провайдерам, посередникам, IT-адміністраторам, користувачам додатків - захищеного доступу до обчислювальних ресурсів, хмарна інфраструктура повинна забезпечувати та передбачати можливість самоврядування і делегування повноважень між користувачами системи[16].

Постачальники хмарних сервісів надають та пропонують послуги декількох фундаментальних моделей:

- Інфраструктура як служба (*IaaS*);
- Платформа як служба (*PaaS*);
- Програмне забезпечення як сервіс (*SaaS*).

Інфраструктура як послуга (*IaaS*) – надання обчислювальних ресурсів за запитом, на яких замовник має можливість розгорнути і запустити довільне програмне забезпечення, що включає в себе операційні системи і додатки (Рис.2.1). В рамках даної моделі замовник не керує і не контролює лежить в основі фізичну інфраструктуру, але має контроль над операційними системами і розгорнутими додатками.

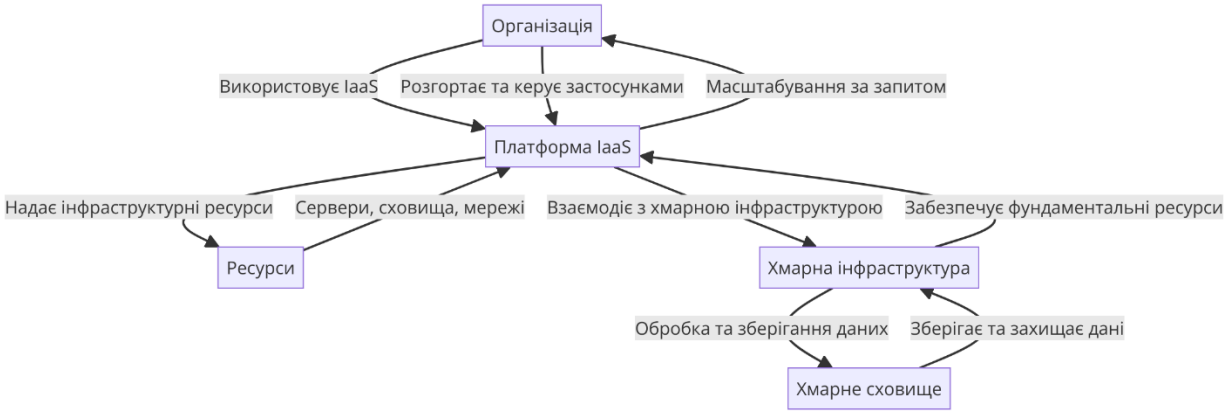

Рис. 2.1. Принцип роботи послуги *IaaS*

Платформа як послуга (*PaaS*) – надання хмарної платформи для розгортання програмного забезпечення, створеного на базі мов програмування і інструментів, які підтримуються хмарним провайдером (Рис.2.2). Замовник не має можливості управляти хмарної інфраструктурою (мережеве та серверне обладнання, СГД, операційними системами), але має контроль над розгорнутими додатками і, можливо, настройками навколишнього середовища.

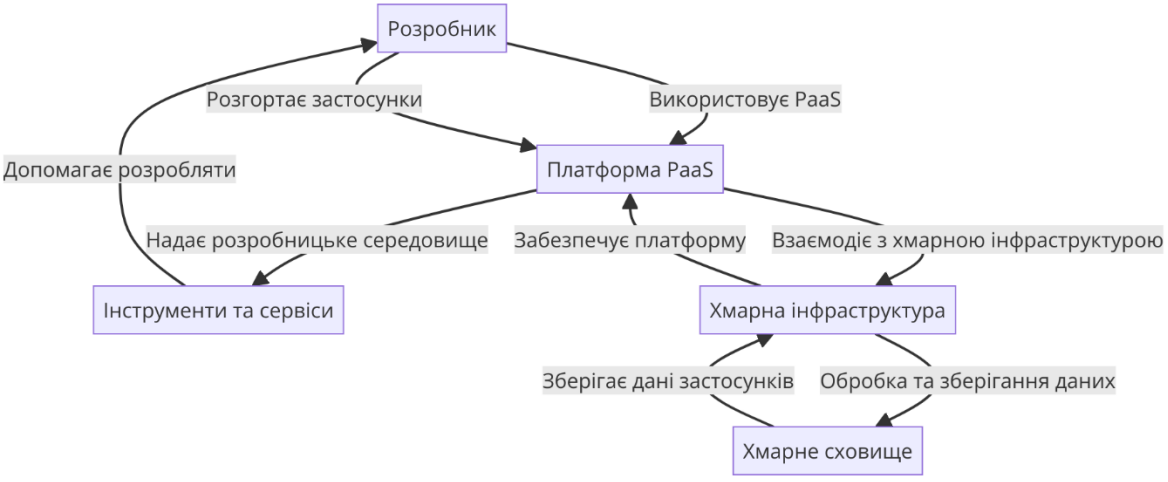

Рис. 2.2. Принцип роботи послуги *PaaS*

Програмне забезпечення як послуга (*SaaS*) – надання в користування замовнику додатків, розгорнутих на хмарної інфраструктурі провайдера (Рис.2.3). Додатки можуть бути доступні з різних клієнтських пристроїв за допомогою тонкого клієнта, термінального клієнта або браузера. Замовник не

контролює параметри роботи і настройки додатків. Весь сервіс надається під ключ.

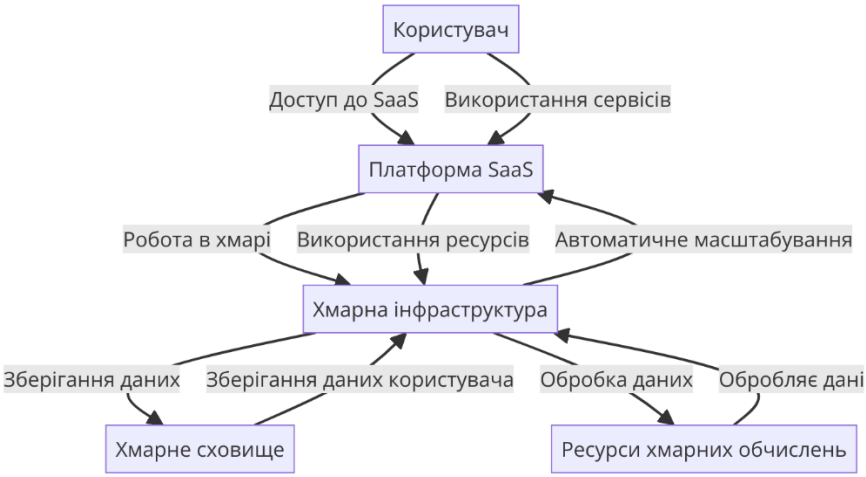

Рис. 2.3. Принцип роботи послуги *SaaS*

2.2 Вибір методів та технологій для реалізації системи виявлення кібератак

Системи безпеки та захисту призначені для виявлення, захисту та відновлення після мережевих атак. Конфіденційність, доступність та цілісність становлять три ключові мети будь-якої системи мережевої безпеки. Методи для виявлення і запобігання вторгненням у мережу можуть бути розподілені залежно від застосованого підходу: виявлення загроз, запобігання їм, або комбінація обох. Ці методи можуть бути реалізовані через програмне забезпечення, апаратні рішення або їх поєднання. Їх можна поділити на два класи: системи виявлення вторгнень і системи запобігання вторгненням [17-18].

Серед основних методів, що використовуються для виявлення кібератак, можна виділити дві основні групи:

- методи сигнатурного аналізу [19, 20];
- методи виявлення аномалій [21, 22].

Тобто, щодо запобігання виявлення кібератак можна віднести системи виявлення вторгнень, виявлення яких працює на основі сигнатур і на основі аномалій, що є двома найпоширенішими підходами, які використовуються системи виявлення вторгнень для виявлення загроз. Сигнатурні процедури

використовуються для ідентифікації лише відомих загроз, орієнтуючись на базу даних з описами характеристик вже відомих атак для виявлення підозрілих дій.

Базу даних необхідно регулярно оновлювати для включення інформації про нові атаки. Перевагою методів сигнатурного аналізу є висока ефективність виявлення відомих атак і мала кількість «помилкових тривог», помилок першого роду. Недоліками таких методів є:

– необхідність постійного поповнення бази знань сигнатурами нових атак, оскільки в іншому випадку існує потенційна небезпека "пропуску атаки", що характеризується помилкою другого роду;

– високі обчислювальні витрати.

З іншого боку, процедури, що базуються на виявленні аномалій, спрямовані на розрізнення зловмисного трафіку від безпечного шляхом аналізу змін у мережевій активності, що дозволяє їм виявляти невідомі загрози. Такі невідповідності, як нехарактерно великий трафік, затримки в мережі, трафік з незвичних портів та аномалії у продуктивності системи, можуть сигналізувати про зміни в звичайній поведінці системи та вказувати на потенційні мережеві атаки. Перевагою методів виявлення аномалій є здатність розпізнавати нові типи атак. Методи виявлення аномалій мають наступні недоліки:

– вимагають тривалого машинного навчання;

– характеризуються низькою ефективністю та високими обчислювальними витратами;

– мають властивість відтворювати помилки першого роду, тобто хибні і невиправдані тривоги, що потребуватиме більш кваліфікованого персоналу для обслуговування.

В сучасних інфраструктурах СВВ є невід'ємною їх частиною. Крім того, до впровадження ШІ традиційний підхід роботи СВВ був здебільшого неефективним у боротьбі з новими та невідомими загрозами (тобто він не був адаптивним), і існує ймовірність того, що він генерує велику кількість хибних спрацьовувань, що може призвести до виснаження ресурсів. Ці традиційні системи безпеки використовують такі інструменти, як *IDS, IPS* і брандмауери

для захисту від простих атак, які повторюють одну і ту ж тактику і інструменти, і реалізовані незалежно один від одного таким чином, що між ними не існує ніякого контакту, який міг би змусити брандмауер, наприклад, заблокувати вторгнення, виявлене в *IDS* [23-24]. Найбільш популярними з систем з відкритим кодом є *Snort, Suricata* і *OSSEC HIDS*, з систем з пропрієтарним кодом *CATNET* і *McAfee IPS*.

Серед популярних МСВВ є *Cisco Secure* IDS, яка інтегрується з міжмережевими екранами, виробленими тією ж компанією, та *Dragon IDS*, гібридна система виявлення вторгнень, що може бути встановлена як на пристрої, так і на робочі станції.

Одним із напрямків розвитку СВВ є інтеграція когнітивних здібностей у їхній функціонал через застосування штучних нейронних мереж та нечіткої логіки. Таке нововведення дозволить значно зменшити кількість помилкових тривог. Цим також і пояснюється значна увага, що приділяється в останні роки, наприклад, квантовій криптографії [25], технології, захищеній блокчейном [26], яка мінімізує часовий проміжок незахищеності мережі.

Також цікавим напрямком в якому спостерігається тенденція є мініатюризації СВВ, що в майбутньому дозволить встановлювати їх на кожен пристрій в мережі, в тому числі на комутатори та свічі, підвищуючи рівень безпеки в цілому.

Останнім часом фокус атак змістився до прикладного рівня моделі *OSI*, зокрема до *SOAP*, *ERP*, *CRM*, баз даних, *IP*-телефонії, веб-сервісів, тощо. Мережеві системи виявлення та запобігання проявили недостатню ефективність проти таких атак, оскільки не працюють на відповідному рівні їх реалізації. Тому, однією з ключових областей розвитку є підтримка нових технологій та протоколів.

Сучасний ринок пропонує багато різних систем виявлення вторгнень. Переглянемо найбільш помітні з них:

– *OSSEC* відноситься до мультиплатформенних маштабованих вузлових систем виявлення вторгнень. Вона має достатнього рівня ефективності

компоненти аналізу містить інтегрованим аналіз логів, перевірку цілісності файлів, централізовані політики, виявлення руткітів, оповіщення в режимі реального часу з активними заходами у відповідь. СВВ працює в більшості операційних систем, широко використовувана. *OSSEC* дуже активно розвивається. Для корпоративний клієнтів існує комерційна підтримка. Даний продукт містить добре задокументовану документацію.

– *Bro* є мережевою системою виявлення вторгнень. Має вихідний відкритий код. Відноситься до систем з пасивною СВВ. Підходить тільки для користувачів unix-подібний операційних систем. На сайті виробника присутні рекомендації, що даний програмний продукт слід використовувати тільки як доповнення до вже встановленої СВВ. Даний продукт містить малоінформативну документацію та не підходить для встановлення в якості першої системи.

– *CATNET* – відноситься до інтелектуальної системи для виявлення, аналізу та реєстрації інцидент, що відбулися в мережі. Містить функціонал для виявлення аномалій та спроби вторгнень мережеву інфраструктури підприємства, контролю подій в інфраструктурі організації. Продукт пропонує достатньо швидкий і ефективний моніторинг мережі, безпеки, журналу подій для подальшого аналізу та має постійну підтримку оновленнями. Випуском *CATNET* займається французька компанія. Даний програмний продукту містить добре задокументовану документацію, проте вона доступна тільки на французькій мові.

– *Snort* – це продукт для виявлення і запобігання вторгнень. Відноситься до продуктів з відкритим вихідним кодом. Початкова система вміла тільки виявляти вторгнення, але потім був добавлений функціонал запобігання вторгнень, що зробило її багатофункціональною системою. Система здатна виконувати в режимі реального часу аналіз трафіку і реєстрацію по ip-мережі. Даний продукт містить добре задокументовану документацію і також за рахунок всесвітньої популярності має досить велику кількість спільнот з підтримки продукту.

Програмні продукти містять документацію. На офіційному сайті розробників можна завантажити керівництво користувача, в якому доступно описано всі можливості даних СВВ і як їх можна конфігурувати. Мова написання власних правил гнучка.

Таблиця 2.1

Порівняльна характеристика систем виявлення вторгнень

СВВ/ Параметр	Bro	CATNET	OSSEC	Snort
Безкоштовна модель поширення	+	-	+	+
Прозорість та відкритість коду	+	-	+	+
Мультиплатформеність	-	+	+	+
Графічний інтерфейс	-	+	+	-
Тип системи	Мережева	Мережева	Вузлова	Мережева, вузлова

2.3 Проектування архітектури системи виявлення кібератак

Технологія хмарних обчислень широко застосовується сьогодні і користується популярністю, проте питання безпеки, що виникають на її фоні, залишаються проблематичними. Користувачі відправляють запити на потрібні дані або ресурси через мережу, що вимагає відповідних безпекових заходів для їх обробки та реагування. Хмарні сервіси, зацікавлені в задоволенні запитів клієнтів, вживають спеціальні заходи для захисту цих запитів. Однак існує ризик, що зловмисники можуть намагатися маніпулювати користувачами, процес, який класифікується як вторгнення і контролюється за допомогою систем виявлення вторгнень (СВВ). У цьому контексті запропонована модель (Рис 2.4) розроблена для того, щоб забезпечити легке та безпечне виконання завдань користувачем у хмарному середовищі.

.

Рис. 2.4. Система виявлення вторгнення у «хмарному» сервісі

У запропонованій моделі СВВ мережевий моніторинг використовується у точках збільшеного навантаження мережі. В цій моделі, для детекції вторгнень, застосовано ВСВВ для стеження за запитами, що відправляються користувачами. Для оптимальної обробки високого трафіку мережі здійснюється багатопоточна обробка даних. Запити, ініційовані з боку кінцевого клієнта, обробляються за допомогою МСВВ, які зареєстровані в СВВ. Багатопоточна модель МСВВ для хмарного середовища заснована на трьох основних модулях: модулі захоплення та обробки запитів, модулі аналізу та модулі звітування. Модуль захоплення виконує функції збору та прийому даних пакетів, включаючи ICMP, TCP, IP, UDP. Оскільки в систему МСВВ надходить велика кількість даних пакетів, модуль спочатку класифікує та організує їх у впорядковану чергу. Потім вибрані пакети передаються як тестові приклади до модулю аналізу (Рис 2.5).

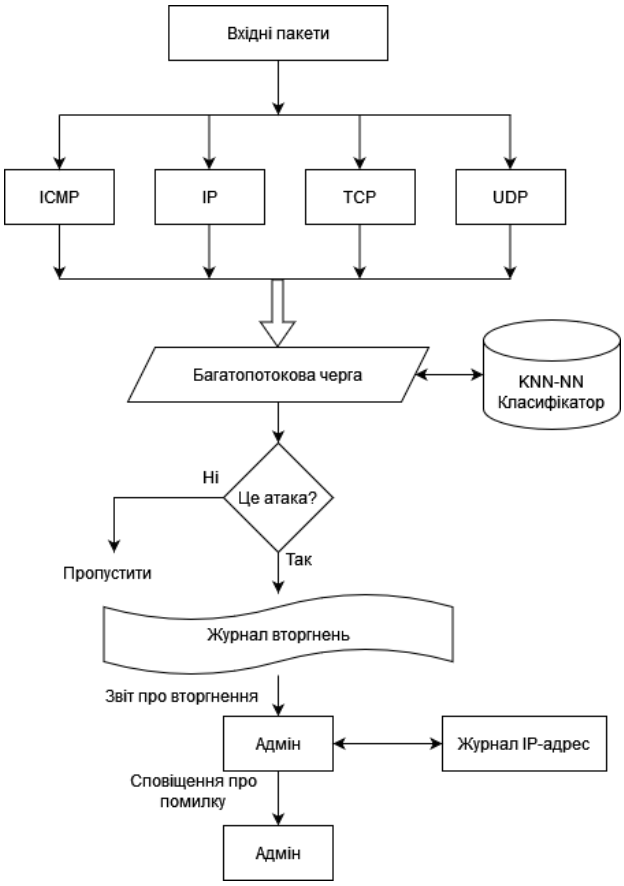

Рис. 2.5. Блок-схема СВВ, що використовує класифікацію *KNN-NN*

Пакети вилучаються з потоку пакетів, що очікують аналіз та переходять до фази аналізу, де їх аналізують за допомогою паралельної обробки кількох потоків. Модуль звітності реагує на результати аналізу та сповіщає адміністратора про виявлені втручання. Всі пакети, призначені для аналізу, систематично обробляються за допомогою класифікатора *KNN-NN*, який було заздалегідь навчено використовуючи набір даних *NSL-KDD* [27]. Пакети, що підпадають під підозрілу поведінку, проходять додатковий аналіз для виявлення потенційних зловмисних активностей. Аналіз ведеться за стандартною процедурою для покращення ефективності системи та оброблення пакетів. Крім того, для кожного вхідного пакета проводиться детекція аномалій за допомогою алгоритму *K-Nearest Neighbor* [27].

Алгоритм може визначати серед наявних для аналізу спостережень k відомих об'єктів (k-найближчих сусідів), які мають ознаки нового, раніше невідомого об'єкту. На основі класів цих найближчих сусідів формулюється

рішення про класифікацію нового об'єкта. Однією з ключових задач алгоритму є вибір коефіцієнта k, що визначає кількість об'єктів, які будуть розглядатися як близькі [27].

На першому етапі роботи алгоритму необхідно визначити кількість k – число найближчих елементів, які будуть відноситись до сусідніх. Якщо встановити k рівним 1, алгоритм може втратити здатність до узагальнення, тобто здатність коректно класифікувати раніше невідомі дані, оскільки новий запис буде класифіковано занадто близько до одного зразка. З іншого боку, занадто велике значення k може призвести до того, що будуть враховані багато локальних особливостей, що може спотворити результати.

На другому етапі алгоритму відбувається процес визначення k записів, які мають найменшу відстань до вектора ознак нового об'єкта. Даний вектор відповідає за процес пошук сусідніх об’єктів за значенням вектору [27]. Функція, що відповідає за розрахунок відстані повинна містити значення, що підходять за наступним правилам та умовам:

− d(x,y) ≥ 0, d(x,y) = 0 Тільки у випадку, коли x дорівнює y.

− d(x,y) = d(y,x);

− d(x,z) ≤ d(x,y) + d(y,z), при умові, що точки x, y, z не розташовані на одній прямій..

Де x, y, z – вектори ознак порівнюваних об'єктів.

Для впорядкованих значень атрибутів обчислюється Евклідова відстань

$$D_E = \sqrt{\sum_i^n (x_i - y_i)^2} \qquad (1)$$

де n – кількість атрибутів.

Для строкових змінних, які не підлягають порядкуванню, застосовується функція відмінності, яка задається наступним чином [27]

$$dd(x,y) = \begin{cases} 0, x = y \\ 1, x \neq y \end{cases} \qquad (2)$$

Також виконується розрахунок нормалізації відстані.

Мінімаксне нормування

$$X^x = \frac{x - \min(x)}{\max(X) - \min(X)} \quad (3)$$

Нормалізація значень за допомогою обрахування стандартного відхилення

$$X^x = \frac{X - X_{cp}}{\sigma_x} \quad (4)$$

де σ_x– стандартне відхилення, Хср – середнє значення.

При визначенні відстані, що дозволяє сприяти зменшенню помилок під час процесів класифікації, застосовується відповідна формула

$$D_E = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \quad (5)$$

Формула для розрахунків багатовимірного простору

$$D_E = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2} \quad (6)$$

Отже, завдяки використанню цього алгоритму допомагає розподіляти дії на «нормальні» та «аномальні». Потім пакети, що пройшли фільтрацію та які класифіковані як «аномальні», аналізуються для виявлення неправильного використання і категоризуються за типами атак. Для навчання класифікатора використовується повний пакет бібліотек *NSL-KDD* [28].

Якщо система виявляє пакети, класифіковані як «аномальні» та їй не вдається віднести їх до конкретних типів атак, система реєструє це як атаку і

створює звіт, вказуючи, що дана атака не ідентифікована в базі даних та додає до звіту примітку «невідома».

Адміністратору надходить звіт про вторгнення, що пройшов через систему класифікації і, виходячи з значенння лічильника подій для кожного втручання, вживає відповідних дій та заходів для забезпечення безпеки.

Адміністратор використовується для управління списком *IP*-адрес у журналах зареєстрованих запитів клієнтів та відповідає за інформацію, що надходить для навчання класифікатора.

Адміністратор вручну проводить навчання системи виявлення вторгнень, аналізуючи звіти про кожну атаку з міткою «невідома». На основі аналізу він відносить події до категорії «нормальний» або «аномальний». Вузлові та мережеві системи виявлення вторгнень, які розміщені у хмарі, використовуються для моніторингу та аналізу користувацьких запитів. У разі виявлення будь-якого запиту на втручання в хмарну систему, протокол вторгнення надходить для аналізу адміністратору для подальших дій.

Отримавши звіт про вторгнення, адміністратор інформує користувача про вторгнення та вносить його до списку IP-журналів. Всі наступні спроби входу будуть контрольовані адміністратором.

Для кожного втручання лічильник подій збільшується на одиницю. Лічильник зі значеннями подій перевіряється щодо встановленого порогового значення. Якщо показник лічильника перевищить цей поріг, доступ для відповідного користувача буде заблокований (Рис 2.6).

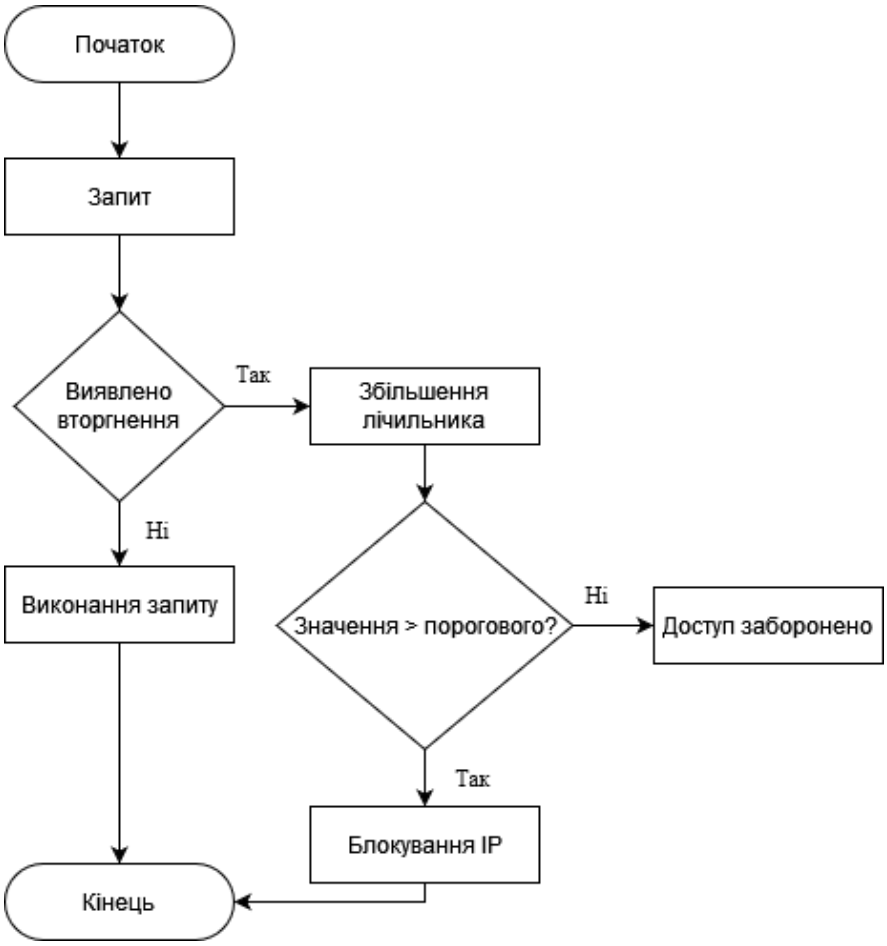

Рис. 2.6. Блок-схема роботи адміністратора

Висновки до розділу 2

Проведена підкреслює важливість подальших досліджень у сфері захисту хмарних сервісів. Розроблена інтелектуальна система автоматичного виявлення мережевих атак може значно підвищити рівень інформаційної безпеки як існуючих, так і майбутніх корпоративних інфраструктур, які інтегрують облачні технології. В запропонованій системі детекції вторгнень реалізовано екстракцію ключових функцій із захоплених пакетів даних для зниження використання пам'яті та часу обробки. Використовуючи гібридний багаторівневий класифікатор KNN-NN, всі пакети класифікуються швидше та ефективніше. Після класифікації адміністратор застосовує заходи для підвищення ефективності системи і виконує дії, спрямовані на тренування класифікатора, категоризуючи поведінку як «нормальну» або «аномальну», що допомагає виявляти атаки чи помилкові спрацьовування.

Розглянута модель може служить ефективним та швидшим підходом для виявлення вторгнення.

Розділ 3 ПРОЕКТУВАННЯ СИСТЕМИ РЕАГУВАННЯ НА КІБЕРАТАКИ

Проектування та впровадження системи реагування в мережеву безпеку МСП здатне зменшити час та потенційну шкоду при забезпечені своєчасного виявлення та реагування на загрози.

Для ефективного проектування. Це передбачає використання програмного та апаратного забезпечення спеціалізованого для моніторингу мережевих з'єднань, аналізу трафіку, виявлення аномалій і підозрілої активності.

3.1.Визначення вимог до системи реагування на кібератаки для малих та середніх підприємств

Система ручного управління дає адміністраторам можливість впроваджувати додаткові заходи безпекового реагування явно. Це дозволяє зменшити шкоду від складних атак, які використовують комбінацію вразливостей, щоб скомпрометувати цільовий комп'ютер [29]. Система ручного управління дозволяє точно контролювати відповіді, але страждає від значних затримок між моментом виявлення проблеми та реагуванням на неї. Натомість автоматизовані системи реагування на вторгнення прагнуть до повної автоматизації, виключаючи необхідність людського втручання у процес прийняття рішень. Це потребує баз з оцінками ризиків, завдяки яким IRS може визначити ймовірність того, що виявлена аномалія є справжньою проблемою та може успішно скомпрометувати свою ціль [30]. Але це в свою чергу генерує проблему, коли для відповіді ризику було вибрано неефективну відповідь для зменшення наслідків атаки, що може статися у разі виникнення складнощів.

Вимоги до системи реагування на кібератаки, яка підходить для МСП, повинні бути ретельно продуманими для забезпечення достатнього захисту від загроз та ефективного реагування на інциденти. Основними аспектами, які слід

врахувати є:

– Збір і моніторинг подій: система повинна бути здатна збирати та контролювати журнали з різних джерел, таких як сервери, робочі станції, мережеві пристрої та IT-сервіси. Це включає в себе інтеграцію з існуючими інфраструктурами, такими як *Active Directory*, *DNS* і *NTP*, для забезпечення безперебійної роботи та узгодженості даних;

– Аналіз і кореляція в реальному часі: він повинен мати можливість виконувати аналіз у реальному часі та кореляцію подій безпеки. Це включає використання попередньо визначених і настроюваних правил кореляції для виявлення потенційних інцидентів безпеки;

– Реагування на інциденти та управління ними: система повинна підтримувати автоматичні механізми реагування, які можуть бути запущені на основі серйозності виявлених інцидентів [31]. Це передбачає інтеграцію з агентами *Windows Event Forwarding* і *WinCollect* для ефективного збору даних і виконання відповіді;

– Управління користувачами та ролями: необхідно підтримувати різні рівні доступу та контролю для різних ролей на підприємстві, наприклад ролі для адміністраторів *SIEM*, аналітиків безпеки та аудиторів. Це допомагає делегувати обов’язки та вдосконалювати внутрішні протоколи безпеки;

– Відповідність і звітність: система повинна забезпечувати комплексні інструменти звітності, які можуть допомогти в управлінні відповідністю та журналах аудиту. Це включає можливість створювати та налаштовувати звіти на основі зібраних даних і результатів аналізу;

– Резервне копіювання та відновлення: необхідні механізми резервного копіювання, щоб забезпечити цілісність і доступність даних, особливо в сценаріях, коли відновлення даних стає необхідним після порушення безпеки;

– Масштабованість та інтеграція: Архітектура повинна підтримувати масштабованість для задоволення зростаючих потреб у безпеці та інтеграцію з

додатковими інструментами та службами безпеки, потенційно включаючи хмарні рішення та програми сторонніх розробників;

– Автоматизований моніторинг працездатності: такі інструменти, як *QRadar Deployment Intelligence*, слід використовувати для моніторингу працездатності та продуктивності системи, забезпечуючи оптимальне функціонування всіх компонентів і швидке вирішення будь-яких потенційних проблем.

Також важливою вимогою до системи буде можливість управління компонентами платформи з одного центрального місця, а також автоматизоване оновлення політик і шаблонів звітності значно спрощують процес аналізу для фахівців з інформаційної безпеки.

3.2.Вибір методів та технологій для реалізації системи реагування на кібератаки

Вибір методів та технологій для реалізації системи реагування на кібератаки має базуватися на комплексному підході, який інтегрує здатність до швидкого аналізу і реагування на інциденти. Використання *SIEM*-систем може ефективно сприяти цьому процесу, адже такі системи забезпечують централізований огляд подій та інцидентів, що дозволяє швидко виявляти та реагувати на потенційні загрози. Система здатна до кореляції даних з різних джерел для виявлення складних атак, які не можуть бути виявлені одномоментно.

Функціонування SIEM системи виконується за допомогою послідовної серії кроків. Спочатку система агрегує дані з різноманітних джерел, потім проводить їх аналіз у режимі реального часу, застосовує профілактичні заходи за необхідності, організовує дані в базах, оцінює активності користувачів на основі раніше зібраної інформації, і, врешті, генерує повідомлення та алерти щодо критичних подій [32].

SIEM системи функціонують через збір та аналіз даних з різних джерел,

таких як журнали подій серверів, аутентифікаційні системи, антивірусні програми та інші засоби моніторингу. Ці системи дозволяють автоматизувати процеси виявлення інцидентів та сприяють швидкому документуванню і інформуванню відповідних служб.

Проаналізуємо наявні на ринку системи, що підходитимуть під наші вимоги:

– *IBM QRadar SIEM*;

– *Splunk*;

– *RSA NetWitness*.

IBM QRadar SIEM відноситься до систем забезпечення повної видимості у мережі підприємства шляхом збору, кореляції та аналізу даних із різних джерел, таких як мережеві пристрої, сервери та програми. Він дуже ефективний у виявленні потенційних загроз безпеці та вразливостей [33]. До ключових особливостей можна віднести:

– інтегровані системи управління відповідністю для допомоги в дотриманні нормативних вимог;

– висока масштабованість, яка адаптується до інфраструктури великих підприємств, що розвивається;

– розширена аналітика для виявлення загроз у реальному часі.

IBM QRadar SIEM підійте для МСП, яким важливо мати потрібен гнучкий аналіз даних різних типів, який можна налаштовувати та використання в середовищах, де необхідна інтеграція з широким спектром програм і форматів даних [33].

Splunk не є суто системою *SIEM*, але пропонує широкі можливості, які можна використовувати для управління інформацією про безпеку та подіями за допомогою потужного механізму збору даних і аналітики. Splunk збирає та індексує дані з журналів, показників, мережевих подій та інших джерел [34]. Ключовими особливостями є:

– настроювані інформаційні панелі та звіти для ефективної статистики;

– розширена аналітика поведінки користувачів для виявлення внутрішніх загроз та інших аномалій з можливістю обробки великих масивів даних із багатьох джерел у реальному часі.

Splunk завдяки універсальними можливостями інтеграції даних і аналітики добре підходить для організацій, які мають справу з величезними обсягами даних з різних джерел.

RSA NetWitness забезпечує виявлення загроз та моніторинг кібербезпеки, аналізуючи дані з журналів, пакетів, кінцевих точок, а також *NetFlow*. Ця система створена для надання глибшого розуміння активності в мережі та на кінцевих точках [34]. До особливостей системи відносяться:

– автоматизоване виявлення загроз у режимі реального часу за допомогою *RSA Live Connect* для постійного оновлення інформації про загрози;

– повна можливість захоплення пакетів, пропонуючи детальну інформацію про мережевий трафік.

Таблиця 3.1

Порівняння різних SIEM систем

Критерій оцінки / Вендор	*IBM QRadar*	*RSA NetWitness*	*Splunk*
Автореєстрація вразливостей	Інтеграція з провідними сканерами великих постачальників, можливість з'єднання через *API* та генерація звітів у різних форматах.	Ні	Інтерграція зі сканерами з відкритих протоколів. Для популярних сканерів є модулі розбору подій
Ризик-кореляція, облік ризик-кореляції у правилах.	Ризик-кореляція з урахуванням складових показника *Magnitude* (*Relevance, Credibility* та *Severity*)	Ні	Модель, яка інтегрує інформацію про активи та користувацькі облікові записи

Продовження таблиці 3.1

Критерій оцінки / Вендор	*IBM QRadar*	*RSA NetWitness*	*Splunk*
Перед настроєні панелі візуалізації та звіти щодо відповідності стандартам (*Compliance*)	*DSS, FISMA, HIPAA, NERC, PCI, COBIT, SOX, GSX-Memo22, GLBA*	*FISMA, FERPA, FFIEC, ISO27002, GLBA,*	Використання платних та безкоштовних доповнень
Довільні формули розрахунку ризиків	Ні	Ні	Вбудовано в мову *SPL*, на який спираються правила кореляції

3.3.Проектування архітектури системи виявлення та реагування на кібератаки

Для проектування архітектури системи виявлення та реагування на кібератаки було вирішено використати *QRadar SIEM*. Цей засіб ефективно виконує функції управління політиками згідно з нормами і стандартами, збирає та аналізує логи, та пропонує передові інструменти для виявлення загроз та реагування. Це рішення побудоване на адаптивній платформі *QRadar Security Intelligence Platform*, яка адаптується до зростання підприємства і його змінюваної інфраструктури, забезпечуючи ефективний і своєчасний моніторинг корпоративної безпеки для МСП [35].

QRadar SIEM збирає дані з таких джерел:

– події системи безпеки, включаючи інформацію від брандмауерів, *VPN*, *IDS/IPS* та інших;

– мережеві події, що включають дані від світчів, роутерів, серверів та хостів;

– моніторинг активності мережі, який відслідковує контекстуальні ідентифікатори протоколів 7-го рівня від мережевого трафіку та додатків;

– моніторинг активності користувачів, включаючи дані з систем управління доступом (*IAM*) та сканерів вразливостей;

– журнали подій додатків, як-от *ERP* системи, системи документообігу, бази даних додатків та адміністративні платформи;

– моніторинг загроз, логів та дотримання політик у режимі реального часу [35].

Інтегруючи різноманітні дані, *QRadar SIEM* підвищує ефективність виявлення та реагування на найновіші загрози. Інформація уніфікується та корелюється для оперативного виявлення, сповіщення та реагування на загрози, які менш спеціалізовані засоби захисту через свої обмеження можуть проігнорувати. Моніторинг за допомогою *QRadar SIEM* дозволяє МСП виявляти складні загрози, включно з внутрішнім шахрайством, непризначеним використанням додатків та багатьма іншими [35].

Зазвичай *SIEM*-система встановлюється над захищеною інформаційною системою, яка складається з архітектури «джерела даних» - «сервер додатків» - «сховище даних». *SIEM*-рішення можуть бути представлені як інтегровані пристрої або як комплекси, що складаються з двох-трьох компонентів. Розподілена архітектура забезпечує високу продуктивність та оптимальні можливості для масштабування, дозволяючи впровадження *SIEM*-рішень в *IT*-інфраструктурах з декількома локаціями.

Архітектура *QRadar SIEM* пропонує різні варіанти імплементації, які підходять для МСП. Найпростіший спосіб розгортання — використання автономного супервізора у форматі "Все-в-одному" (Рис.3.1) [36]. В цьому випадку один супервізор виконує всі завдання: збір, моніторинг, аналіз та обробку даних, а також відстеження інцидентів безпеки. Для покращення точності моніторингу на робочих станціях та серверах можна використовувати WinCollect Agent(s) [37-38].

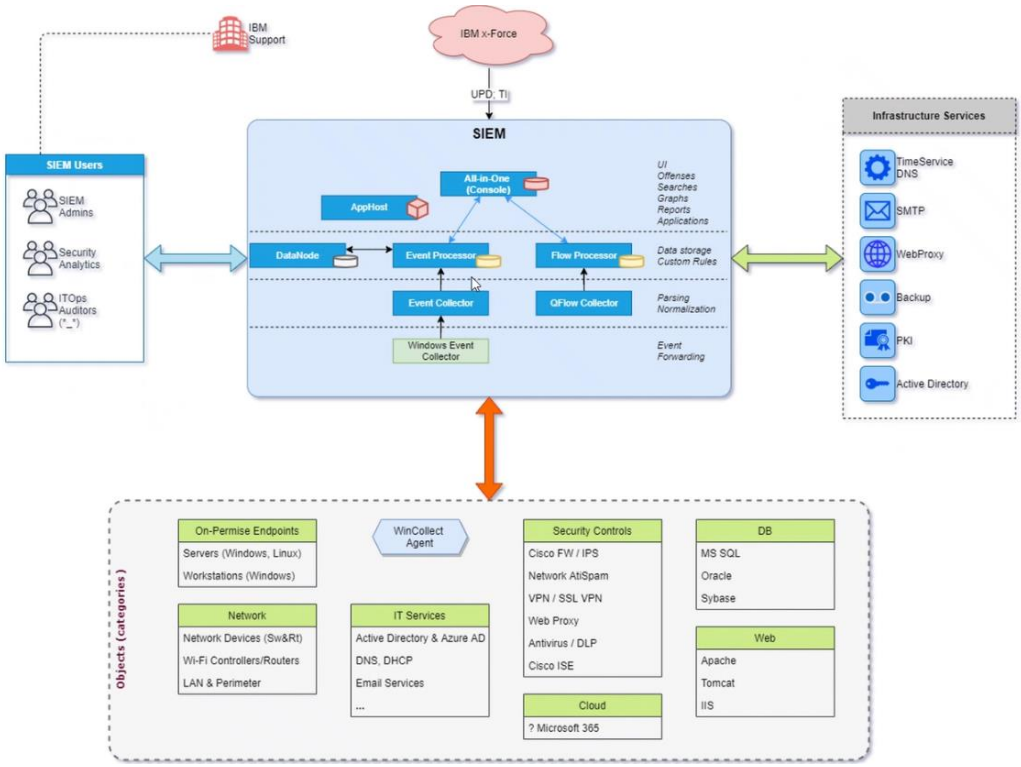

Рис. 3.1. Верхньорівнева архітектура *QRadar SIEM*

Схема застосування *QRadar SIEM* представлена рисунку 3.2. Дана архітектура впровадження системи *QRadar SIEM* в інфраструктуру підприємства, включаючи інтеграцію з ключовими компонентами мережі та серверами. Архітектура охоплює різні джерела даних, від серверів і робочих станцій до спеціалізованих інструментів моніторингу, забезпечуючи всебічний підхід до управління інцидентами безпеки. Метою схеми є надання зрозумілої візуалізації способу інтеграції *QRadar SIEM* в існуючу IT-інфраструктуру підприємства, що включає як *Linux*, так і *Windows* екосистеми, з особливим акцентом на ефективне збирання та обробку даних для швидкого виявлення та реагування на інциденти [38].

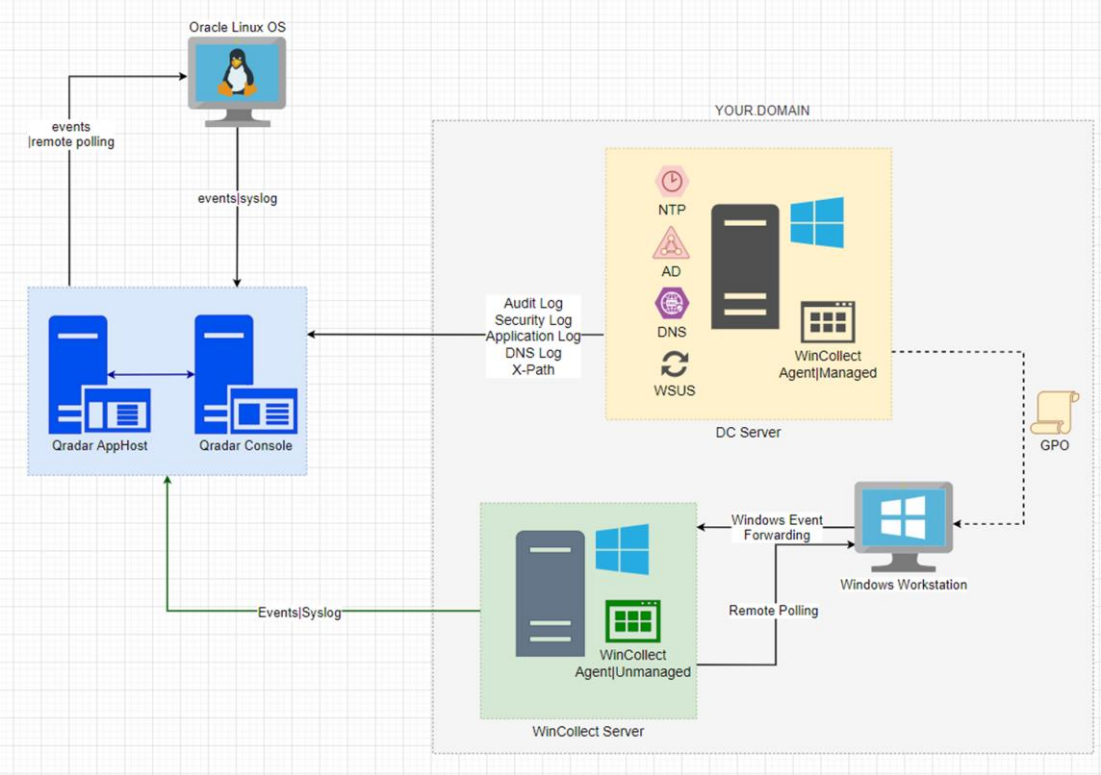

Рис. 3.2. Інтеграції *QRadar SIEM* в систему мережевої безпеки підприємства

За розробленою схемою (Рис.3.2) було розгорнуто QRadar SIEM Console та QRadar SIEM Apphost, що є ключовими компонентами системи безпеки МСП.

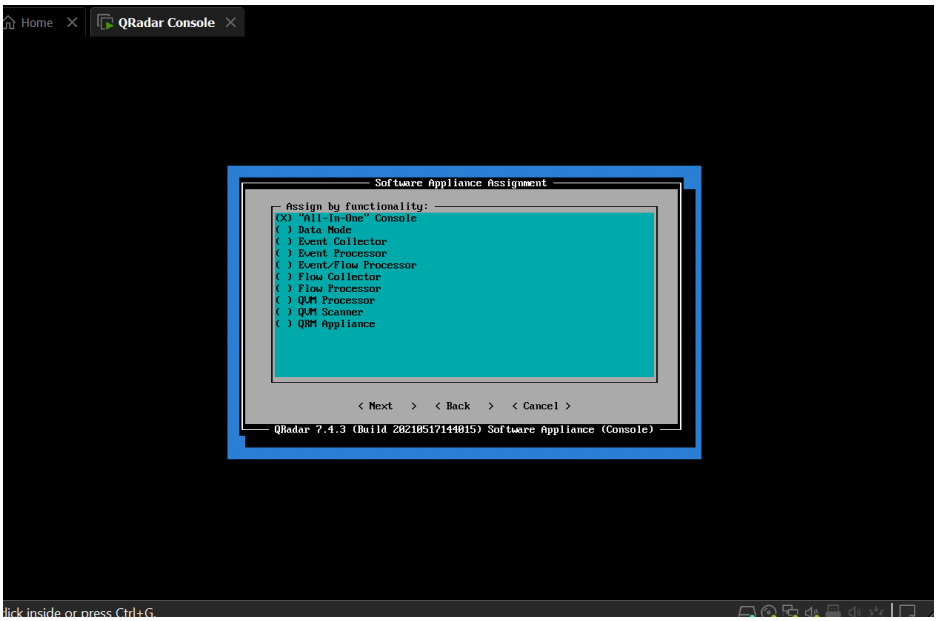

Рис. 3.3. Початок інсталяції *QRadar Console*

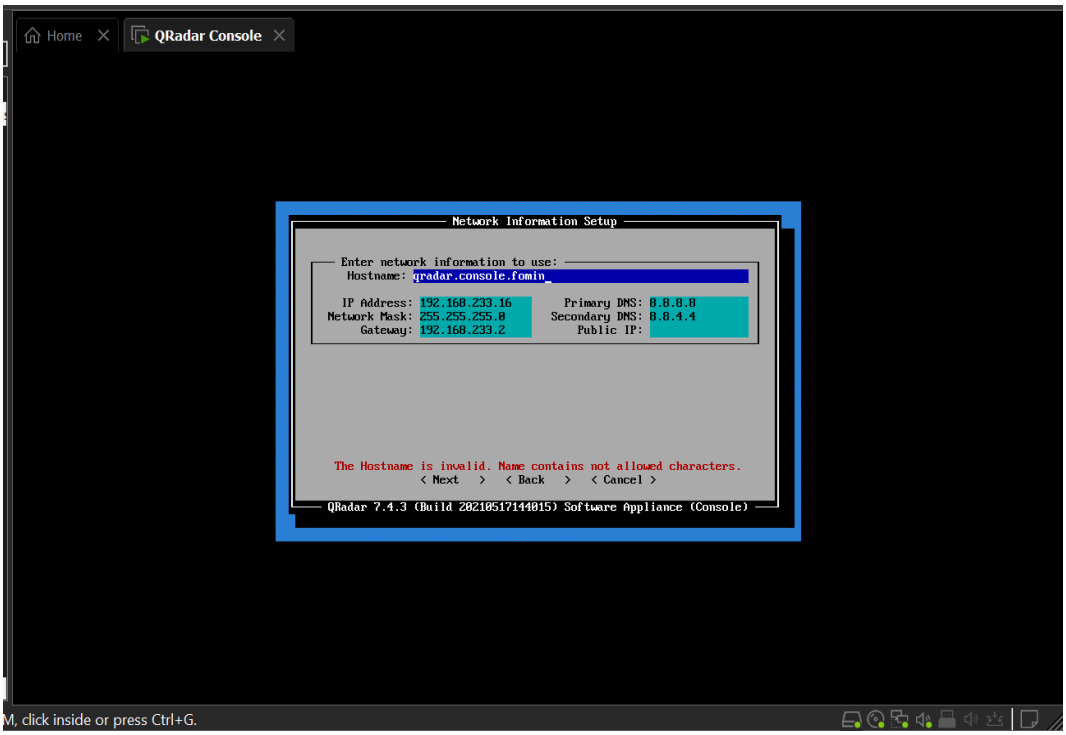

Рис. 3.4. Налаштування мережевого інтерфейсу *QRadar Console*

Під час налаштування мережевого інтерфейсу *QRadar Console* (Рис.3.4) вводимо ім’я хоста, *IP*-адреси (*IPV4*), маску мережі, шлюз за замовчуванням і інформацію про *DNS* [39].

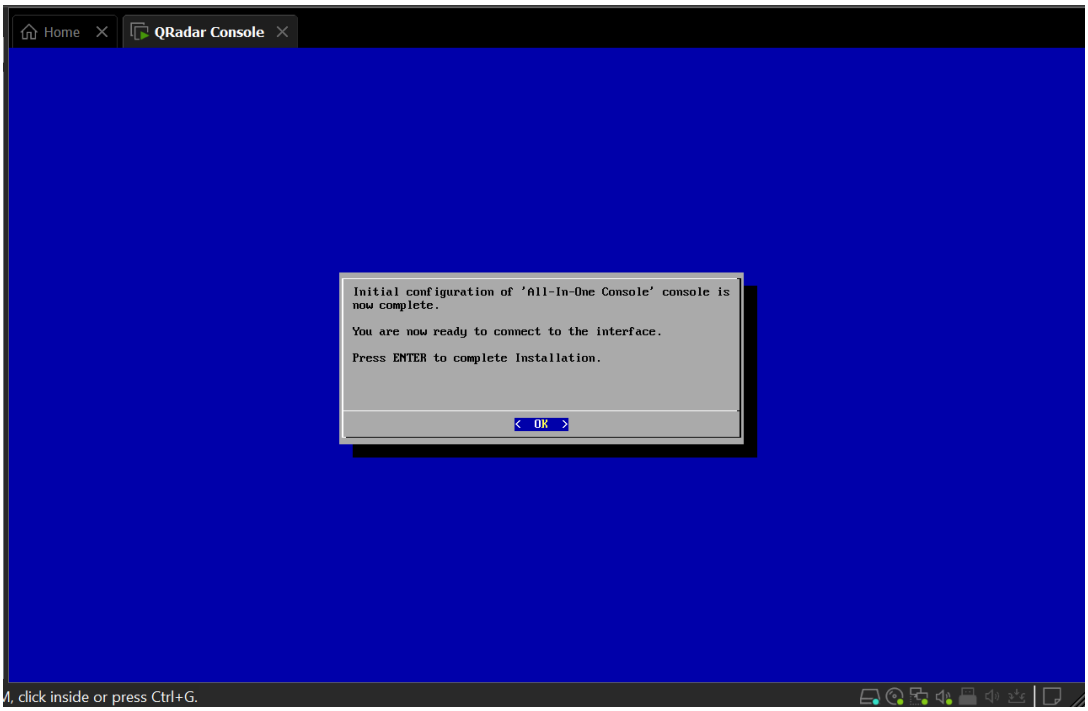

Рис. 3.5. Завершення інсталяції *QRadar Console*

Після інсталяції (Рис.3.5) в інтерфейс *QRadar Console*, налаштовуємо політики безпеки, мережеві ієрархії, розгортаємо додаткові вузли даних, якщо це необхідно, і інтегруємо з іншими системами або програмами.

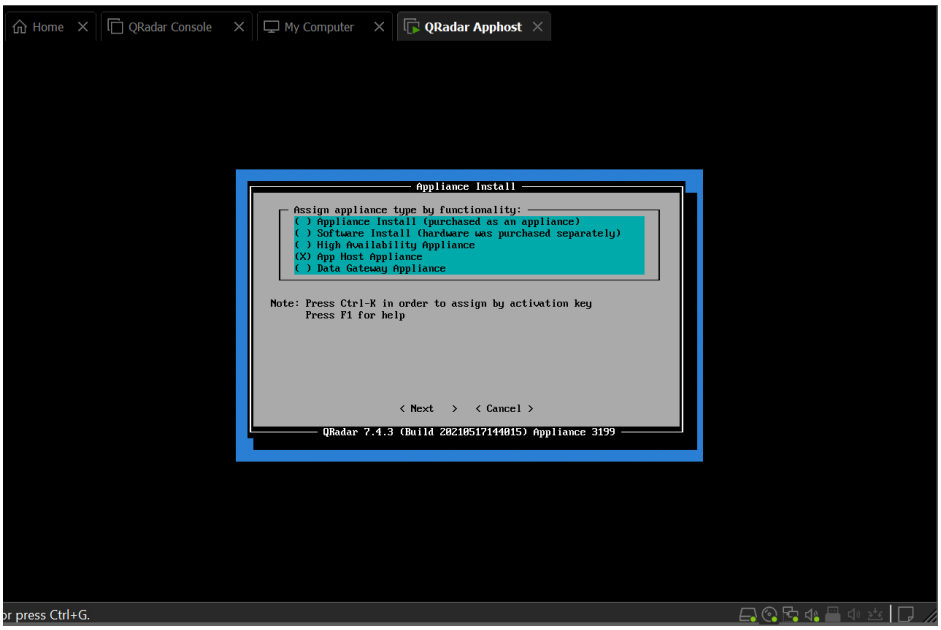

Рис. 3.6. Початок інсталяції *QRadar Apphost*

Під час інсталяції налаштування мережевого інтерфейсу *QRadar Apphost* (Рис.3.7) вводимо ім’я хоста, *IP*-адреси (*IPV4*), маску мережі, шлюз за замовчуванням і інформацію про *DNS*.

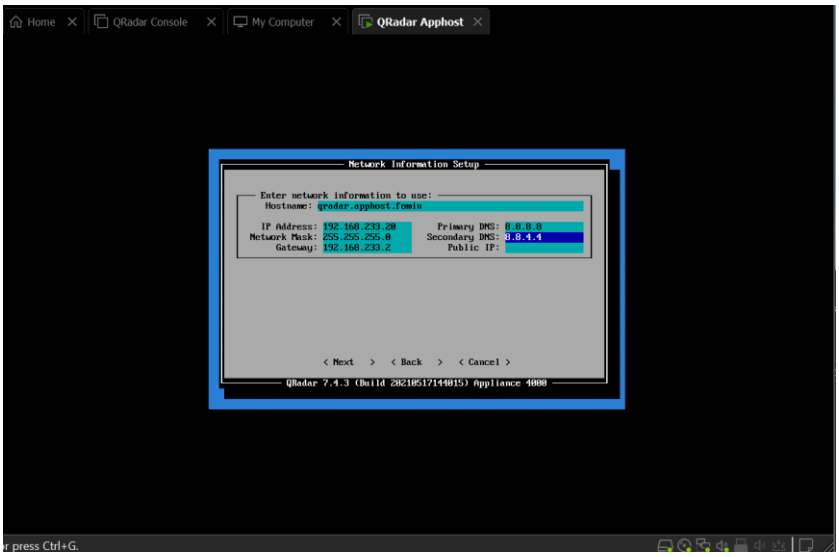

Рис. 3.7. Налаштування мережевого інтерфейсу *QRadar Apphost*

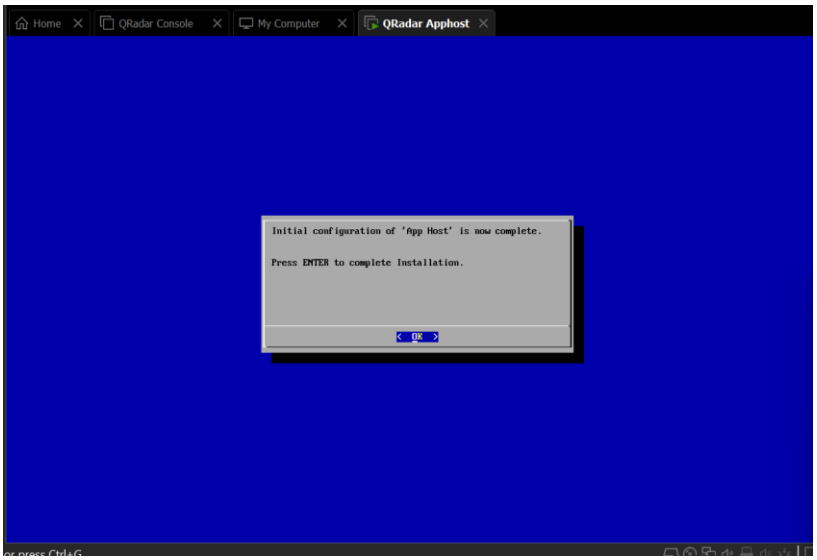

Рис. 3.8. Завершення інсталяції *QRadar Apphost*

Після інсталяції (Рис.3.8) *QRadar Apphost* переходимо в налаштування *QRadar Console* та інтегруємо *QRadar Apphost* з *QRadar Console*. Це дозволить розгортати на QRadar Console ресурсоємні додатки, щоб зменшити навантаження на основну систему, забезпечуючи більш ефективне управління ресурсами та покращуючи загальну продуктивність системи [40]. Ця стратегія відіграє ключову роль у оптимізації процесів обробки даних і аналізу, дозволяючи основній системі зосередитись на критично важливих задачах безпеки (Рис.3.9).

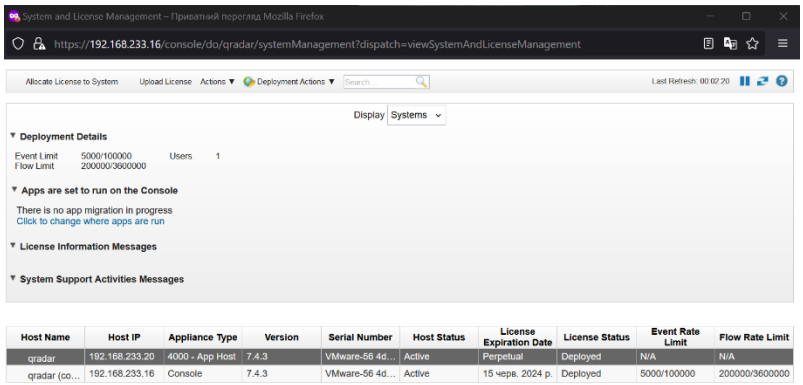

Рис. 3.9. Інтеграція *QRadar Apphost* з *QRadar Console*

Висновки до розділу 3

У третьому розділі було спроектовано архітектуру системи реагування на кібератаки для малих та середніх підприємств. Основною метою цього розділу було визначення вимог до системи, вибір відповідних методів та технологій, а також розробка архітектури системи, здатної ефективно реагувати на сучасні кіберзагрози.

Протягом аналізу було з'ясовано, що малі та середні підприємства стикаються з унікальними викликами у забезпеченні кібербезпеки через обмежені ресурси та високий рівень вразливості до кібератак. Це вимагає знаходження гнучких та економічно вигідні рішення, що могли б адаптуватися до змінюваних умов загрози та водночас бути доступними для реалізації на МСП.

В ході розробки архітектури системи реагування на кібератаки було розглянуто інтеграцію засобів автоматичного виявлення аномалій, а також методів швидкого реагування, які можуть значно скоротити час від моменту виявлення атаки до моменту її нейтралізації. Розглянули різноманітні технологічні рішення, які допомагають забезпечити глибинний аналіз даних та ефективне реагування на інциденти безпеки.

Основним результатом роботи стало формулювання практичних рекомендацій для підприємств, що включають в себе кроки з впровадження та налаштування системи, що дозволить їм не тільки реагувати на поточні загрози, а й прогнозувати можливі кібератаки в майбутньому, забезпечуючи тим самим вищий рівень захисту інформаційних активів.

Таким чином, розроблена система реагування на кібератаки стане надійним інструментом у підвищенні рівня кібербезпеки малих та середніх підприємств, зменшуючи ризики втрати даних та фінансових збитків від потенційних інформаційних загроз.

ВИСНОВКИ

Під час роботи над дипломним проектом було виконано поставлені завдання:

1. Досліджено особливості кіберзагроз для малих та середніх підприємств та встановлено, яким загрозам кібербезпеки піддаються малі та середні підприємства, аналізуються існуючі методи і технології виявлення та реагування на кібератаки.

2. Проаналізовано сучасні методи та технології виявлення та реагування на кібератаки, та виявлено, що інтеграція SIEM систем дозволяє виявляти та реагувати на загрози за рахунок їх здатності до централізації логів та подій з усіх частин IT-інфраструктури підприємства.

3. Проведено пілотне тестування, що підтвердило ефективність розробленої системи у виявленні та реагуванні на загрози.

4. В ході роботи розроблено схему впровадження *QRadar SIEM* систему безпеки підприємств, яка відрізняється від відомих тим, що має відображення взаємодії серверів, робочих станцій та служб, і те як вони взаємодіють у мережі.

5. Наведено приклад розгортання системи та проведено пілотне тестування, яке підтвердило дієздатність розробленої системи у виявленні та реагуванні на загрози за рахунок розгортання цієї системи на кафедрі управління інформаційною та кібернетичною безпекою університету.

Завдяки простоті інтерфейсу, *QRadar SIEM* може бути використаний як досвідченими користувачами, так і молодими спеціалістами служби інформаційного та кібернетичного захисту у структурах малих та середніх підприємств (організацій).

Мету проекту було досягнуто. Підвищення рівня кіберзахисту малих та середніх підприємств за допомогою впровадження розробленої системи виявлення та реагування на кібератаки, з можливістю її вдосконалення у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A.Vives, ‘‘Social and environmental responsibility in small and medium enterprises in Latin America,’’ (in English) J. Corporate Citizenship, vol. 2006, no. 21, pp. 39–50, Mar. 2006. DOI: http://dx.doi.org/10.9774/GLEAF.4700.2006.sp.00006 (дата звернення: 01.04.2024).

2. Data Breach Statistics 2023. URL: https://www.varonis.com/blog/data-breach-statistics (дата звернення: 02.04.2024).

3. Impact of Information Security Threats on Small Businesses During the Covid-19 Pandemic. URL: https://www.researchgate.net/publication/361314523 (дата звернення: 02.04.2024).

4. Verizon 2023 Data Breach Investigations Report. URL: https://www.verizon.com/business/en-nl/resources/reports/dbir/ (дата звернення: 02.04.2024).

5. Rawindaran, N.; Jayal, A.; Prakash, E.; Hewage, C. Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME). Future Internet 2021, 13, 186. DOI: https://doi.org/10.3390/fi13080186 (дата звернення: 03.04.2024).

6. Saber Mhiri. SIEM For industrial SME: needs and the obstacles URL: https://www.inprosec.com/wp-content/uploads/2019/09/SIEMS_for_SME.pdf (дата звернення: 03.04.2024).

7. Endpoint Detection and Response (EDR) – A Must-Have for SMEs URL: https://gxait.com/business-strategy/endpoint-detection-and-response-edr-a-must-have-for-smes/ (дата звернення: 05.04.2024).

8. Ike Vayansky and Sathish Kumar. Phishing – challenges and solutions DOI: https://doi.org/10.1016/S1361-3723(18)30007-1 (дата звернення: 07.04.2024).

9. Stavros, Jacqueline & Saint, Daniel. (2010). SOAR: linking strategy and od to sustainable performance. URL: https://www.researchgate.net/publication/285056921 (дата звернення: 08.04.2024).

10. Using a SOAR analysis to enhance your strategic planning URL:https://www.notion.so/blog/soar-analysis (дата звернення: 07.04.2024).

11. Elezaj, Ogerta & Yildirim Yayilgan, Sule & Abomhara, Mohamed & Yeng, Prosper & Ahmed, Javed. (2019). Data-Driven Intrusion Detection System for Small and Medium Enterprises. 1-7. 10.1109/CAMAD.2019.8858166.URL: https://www.researchgate.net/publication /336336559 (дата звернення: 10.04.2024).

12. How to response to a Cyber Attack. URL: https://www.nist.gov/blogs/ manufacturing-innovation-blog/how-respond-cyber-attack (дата звернення: 13.04.2024).

13. Cybersecurity Incident Response Guide. URL: https://mattermost.com/ cybersecurity-incident-response-guide/#best-practices-for-cybersecurity-incident-response (дата звернення: 13.04.2024).

14. Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Cogent Engineering, 10(2). DOI: https://doi.org/10.1080/23311916.2023.2272358 (дата звернення: 14.04.2024).

15. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2021. 256 с. (дата звернення: 15.04.2024).

16. І.І. Єніна, доц., канд. техн. наук, А.С. Мороз, ст. гр. СІ-13. Перспективи застосування хмарних технологій для зберігання інформації (дата звернення: 15.04.2024). С.1-3 . (дата звернення: 15.04.2024).

17. Rahman R.U., Tomar D.S. Emerging Wireless Communication and Network Technologies: Principle, Paradigm and Performance. Springer; Singapore: 2018. Security attacks on wireless networks and their detection techniques; pp. 241–270. (дата звернення: 16.04.2024).

18. Azeez N.A., Bada T.M., Misra S., Adewumi A., der Vyver C., Ahuja R. Intrusion Detection and Prevention Systems: An Updated Review. In: Sharma N., Chakrabarti A., Balas V.E., editors. Data Management, Analytics and Innovation. Springer; Singapore: 2020. pp. 685–696. (дата звернення: 16.04.2024).

19. Toliupa, S. Signature and statistical analyzers in the cyber attack detection system / S. Toliupa, V. Nakonechnyi, O. Uspenskyi // Information Technology and Security. – 2019. – Vol. 7, Iss. 1(12). – P. 69–79. (дата звернення: 17.04.2024).

20. Snehi, J. Diverse Methods for Signature based Intrusion Detection Schemes Adopted / J. Snehi // International Journal of Recent Technology and Engineering. – 2020. – Vol. 9, Iss. 2. – P. 44-49. (дата звернення: 17.04.2024).

21. Ananin, E. Anomalies and intrusions detection methods / E. Ananin, I. Kozhevnikova, A. Lysenko, A. Nikishova // Problems of Science. – 2016. – No. 34 (76). – P. 48-50. (дата звернення: 17.04.2024).

22. Manasi, G. Taxonomy of Anomaly Based Intrusion Detection System: A Review / G. Manasi // International Journal of Scientific and Research Publications. – 2012. – Vol. 2, Iss. 12. – URL: http://www.ijsrp.org/research-paper-1212.php?rp=P12460. (дата звернення: 18.04.2024).

23. El Kamel, N., Eddabbah, M., Lmoumen, Y. and Touahni, R. 2020. A smart agent design for cyber security based on honeypot and machine learning. Hindawi, Security and Communication Networks Volume 2020, Article ID 8865474: 1-9. DOI: https://doi.org/10.1155/2020/8865474 (дата звернення: 18.04.2024).

24. Nweke, Chidiebere & Eze, Paulinus & Ezenugu, Isaac & Okorogu, Victor. (2024). Methods, Potentials and Challenges of Machine Learning Based Artificial Intelligence Systems in Cyber Security. 91-107. URL: https://www.researchgate.net/publication/379258759 (дата звернення: 18.04.2024)

25. Hibrid quantum random number generator for cryptographic algorithms / M. Iavich, T. Kuchukhidze, G. Lashvili, S. Gnatyuk //Radioelectronic and computer systems, – 2021. – No. 4. – P. 103-118. DOI:10.32620/reks.2021.4.09. (дата звернення: 18.04.2024).

26. Bhardwaj, A. Security Incidents & Response Against Cyber Attacks / A. Bhardwaj, V. Sapra. – Springer, 2021. – 250 p. (дата звернення: 18.04.2024).

27. Марченко О.О., Россада Т.В. Актуальні проблеми Data Mining: Навчальний посібник для студентів факультету комп’ютерних наук та кібернетики (дата звернення: 19.04.2024).

28. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A.: A detailed analysis of the KDD Cup 99 data set. In: Proceedings of the IEEE Symposium on Computational Intelligence in Security and Defense Application (CISDA). pp. 53–58. IEEE Publisher (2009) (дата звернення: 19.04.2024).

29. Noel, S., Wang, L., Singhal, A., Jajodia, S.: Measuring security risk of networks using attack graphs. International Journal of Next-Generation Computing. 1(1), 135-147 (2010) (дата звернення: 21.04.2024).

30. Mu, C. P., Li, X. J., Huang, H. K., Tian, S. F.: Online risk assessment of intrusion scenarios using D-S evidence theory. Proceedings of the 13th European Symposium on Research in Computer Security, pp. 35-48. Springer, Malaga, Spain (2008) (дата звернення: 21.04.2024).

31. Що таке реагування на інциденти? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-incident-response (дата звернення: 23.04.2024).

32. X. Li, X. Zheng, J. Li and S. Wang, "Frequent itemsets mining in network traffic data", Proceedings of the 2020 5th International Conference on Intelligent Computation Technology and Automation ICICTA ‘2020. URL: https://www.researchgate.net/publication/254050608 (дата звернення: 25.04.2024).

33. Heine, Felix. (2017). Outlier Detection in Data Streams Using OLAP Cubes. 29-36. URL: https://www.researchgate.net/publication/319639271 (дата звернення: 25.04.2024).

34. NetWitness Platform. URL: https://www.netwitness.com/solutions/evolved-siem (дата звернення: 26.04.2024).

35. C. C. Aggarwal, Outlier Analysis. in Data Mining: The Textbook, Cham:Springer International Publishing, pp. 237-263, 2019. URL: http://pzs.dstu.dp.ua/DataMining/bibl/Data%20Mining%20The%20Textbook.pdf (дата звернення: 26.04.2024).

36. IBM Security QRadar WinCollect User Guide. URL: http://ftpmirror. your.org/pub/misc/ftp.software.ibm.com/software/security/products/qradar/document

s/71MR1/NAD/Core/WinCollect_UserGuide-71MR1.pdf (дата звернення: 28.04.2024).

37. SIEM система IBM QRADAR як складова SOC наступного покоління. URL: https://conf.ztu.edu.ua/wp-content/uploads/2023/02/92.pdf (дата звернення: 01.05.2024).

38. IBM Security QRadar SIEM – Overview. IBM. URL: https://www.ibm.com/products/qradar-siem. (дата звернення: 04.05.2024).

39. IBM QRadar Installation Guide. URL: https://www.ibm.com/docs/en/ SS42VS_7.4/pdf/b_siem_inst.pdf

40. IBM QRadar Architecture and Deployment Guide. URL: https://www.ibm.com/docs/en/ SS42VS_7.4/pdf/b_siem_deployment.pdf (дата звернення: 04.05.2024).