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: “ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНИМ МЕРЕЖАМ ПІДПРИЄМСТВА”

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

_____ Данило Пічкур
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Данило Пічкур
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна Мужанова
к.держ.упр., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:
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

Пічкуру Данилу Сергійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Технологій виявлення загроз інформаційним мережам підприємства”,
керівник кваліфікаційної роботи МУЖАНОВА Тетяна, к.держ.упр., доцент,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджена наказом Державного університету інформаційно-комунікаційних технологій від “27“ лютого 2024 р. № 36.

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

3. Вихідні дані до кваліфікаційної роботи: *безпека інформаційних мереж підприємства, загрози інформаційним мережам підприємства, технології виявлення загроз інформаційним мережам підприємства.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити основи мережевої безпеки підприємства, зокрема методи та технології запобігання і протидії мережевим загрозам.
4.2. Проаналізувати технології виявлення загроз безпеці мережі (IDS/IPS, EDR, SIEM).
4.3. Оцінити ефективність технологій виявлення загроз мережевій безпеці й розробити практичні рекомендації щодо їх застосування на підприємстві.
Перелік ілюстративного матеріалу: презентація PowerPoint

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Дослідження основ мережевої безпеки підприємства.	08.04.2024	
4.	Аналіз технологій виявлення загроз безпеці мережі (IDS/IPS, EDR, SIEM).	22.04.2024	
5.	Оцінювання ефективності технологій виявлення загроз мережевій безпеці й розробка практичних рекомендацій щодо їх застосування на підприємстві.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Данило ПІЧКУР
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Пічкур Д.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Технології виявлення інформаційним мережам підприємства"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ПІЧКУР Данило у кваліфікаційній роботі дослідив основи мережевої безпеки підприємства, зокрема методи та технології запобігання і протидії мережевим загрозам; проаналізував технології виявлення загроз безпеці мережі (IDS/IPS, EDR, SIEM); оцінив ефективність технологій виявлення загроз мережевій безпеці й розробив практичні рекомендації щодо їх застосування на підприємстві.

У процесі підготовки кваліфікаційної роботи ПІЧКУР Данило показав якісну теоретичну і практичну підготовку, розуміння проблеми дослідження та вміння самостійно знаходити шляхи її вирішення, володіння науково-дослідницькими методами. Результати дослідження апробовані на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 28 лютого 2024 року.

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

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

"____"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Пічкур Д.С. 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 ПІЧКУРА Данила
на тему “Технології виявлення загроз інформаційним мережам підприємства”

Актуальність. У сучасному цифровому світі, де ІТ є основою більшості підприємств, захист інформаційних мереж стає ключовим завданням. Зростання кібератак і складності загроз вимагає впровадження передових технологій для їх виявлення та нейтралізації. Корпоративні мережі містять критичні дані, що потребують надійного захисту. Технології виявлення загроз, такі як IDS/IPS, EDR та SIEM, є невід'ємною частиною ефективної мережевої безпеки. Їх впровадження допомагає оперативно виявляти та реагувати на кіберзагрози, мінімізуючи збитки та забезпечуючи стійкість бізнес-процесів.

З огляду на зазначене дослідження технологій виявлення загроз інформаційним мережам підприємства є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено основні технології запобігання і протидії мережевим загрозам, в тому числі виявлення загроз (IDS/IPS, EDR, SIEM), дано оцінку їх ефективності й представлено практичні рекомендації.

2. Оформлення кваліфікаційної роботи відповідає встановленим вимогам. Текст викладено послідовно, висновки відповідають змісту дослідження, основні положення представлені на рисунках і в таблицях.

3. Автор опрацював значну джерельну базу, переважно англомовну, зокрема описи програмних рішень розвідки загроз від виробників, аналітику щодо ефективності досліджених програмних продуктів.

4. За результатами дослідження зроблено висновок про необхідність застосування інтегрованого підходу до забезпечення мережевої безпеки, зокрема й виявлення загроз мережі для забезпечення багаторівневого захисту.

Недоліки.

Доцільно було б звернути більше уваги на дослідження конкретних програмних продуктів для виявлення загроз мережевй безпеці, порівнянню їх фнкціональності.

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 ПІЧКУР Данило заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

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

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технологій виявлення загроз інформаційним мережам підприємства. Робота складається зі вступу, трьох розділів, що містять 15 рисунків і 2 таблиці, висновків і списку використаних джерел із 42 найменувань. Загальний обсяг роботи становить 73 аркуші, з яких 6 аркушів займають перелік умовних скорочень і список використаних джерел.

Метою роботи є дослідження технологій виявлення загроз інформаційним мережам підприємства.

Об'єктом дослідження є забезпечення безпеки інформаційних мереж підприємства.

Предмет дослідження **–** технології виявлення загроз інформаційним мережам підприємства.

Методи дослідження**.** Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, класифікації і порівняння, експертної оцінки, системного підходу й оцінювання ефективності.

Як результат у роботі досліджено основи мережевої безпеки підприємства, зокрема методи та технології запобігання і протидії мережевим загрозам; проаналізовано технології виявлення загроз безпеці мережі (IDS/IPS, EDR, SIEM); дано оцінку ефективності технологій виявлення загроз мережевій безпеці й розробити практичні рекомендації щодо їх застосування на підприємстві.

Галузь застосування**.** Розроблені підходи можуть бути використані при плануванні та впровадженні комплексу заходів і технологій для підвищення ефективності виявлення загроз мережевій безпеці підприємства.

Ключові слова: БЕЗПЕКА ІНФОРМАЦІЙНИХ МЕРЕЖ, ЗАГРОЗИ ІНФОРМАЦІЙНИМ МЕРЕЖАМ ПІДПРИЄМСТВА, ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНИМ МЕРЕЖАМ ПІДПРИЄМСТВА.

ABSTRACT

The qualification work is dedicated to the study of threat detection technologies for enterprise information networks. The work consists of an introduction, three chapters containing 15 figures and 2 tables, conclusions, and a list of references with 42 items. The total volume of the work is 74 pages, of which 6 pages are occupied by a list of abbreviations and the list of references.

The purpose of the study is to investigate threat detection technologies for enterprise information networks.

The object the study is the security of enterprise information networks.

The subject of the study is the threat detection technologies for enterprise information networks.

Research methods. To solve the above-mentioned scientific task, methods of analysis, comparison and classification, expert evaluation, systematic approach, and effectiveness evaluation were used in the work.

As a result, the work investigates the basics of enterprise network security, in particular, methods and technologies for preventing and countering network threats; analyzes threat detection technologies for network security (IDS/IPS, EDR, SIEM); evaluates the effectiveness of threat detection technologies for network security and develops practical recommendations for their application in an enterprise.

Field of application**.** The developed approaches can be used in the planning and implementation of a set of measures and technologies to increase the effectiveness of detecting threats to the network security of an enterprise.

Keywords: INFORMATION NETWORK SECURITY, THREATS TO ENTERPRISE INFORMATION NETWORKS, THREAT DETECTION TECHNOLOGIES FOR ENTERPRISE INFORMATION NETWORKS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AI	Artificial Intelligence
APT	Advanced Persistent Threat
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS/DDoS	Denial of Service/Distributed Denial of Service
DLP	Data Loss Prevention
DPI	Deep Packet Analysis
EDR	Endpoint Detection and Response
HIDS	Host Intrusion Detection System
HIPS	Host Intrusion Prevention System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MFA	Multi-Factor Authentication
MitM	Man-in-the-Middle
ML	Machine Learning
NAC	Network Access Control
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NTA	Network Traffic Analysis
ROI	Return on Investment
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
TCO	Total Cost of Ownership
TTD	Time to Detect
TTR	Time to Respond
VPN	Virtual Private Network
XDR	Extended Detection and Response

ВСТУП

Актуальність теми. У сучасному цифровому світі, де інформаційні технології є основою більшості підприємств, захист інформаційних мереж стає ключовим завданням. Зростання числа кібератак і складності загроз вимагає впровадження передових технологій для їх виявлення та нейтралізації. Інформаційні мережі підприємств містять критичні дані, що потребують надійного захисту для збереження конфіденційності, цілісності та доступності.

Технології виявлення загроз, такі як IDS/IPS, EDR та SIEM, є невід'ємною частиною ефективної безпеки мережі. Їх впровадження допомагає оперативно виявляти й реагувати на кіберзагрози, мінімізуючи збитки та забезпечуючи стійкість бізнес-процесів.

З огляду на зазначене дослідження технологій виявлення загроз інформаційним мережам підприємства є актуальним науковим завданням.

Мета роботи полягає у дослідженні технологій виявлення загроз інформаційним мережам підприємства.

Об'єкт дослідження **–** забезпечення безпеки інформаційних мереж підприємства.

Предмет дослідження – технології виявлення загроз інформаційним мережам підприємства.

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

1. Дослідити основи мережевої безпеки підприємства, зокрема методи та технології запобігання і протидії мережевим загрозам.

2. Проаналізувати технології виявлення загроз безпеці мережі (IDS/IPS, EDR, SIEM).

3. Оцінити ефективність технологій виявлення загроз мережевій безпеці й розробити практичні рекомендації щодо їх застосування на підприємстві.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, класифікації і порівняння, експертної оцінки, системного підходу та оцінювання ефективності.

Практичне значення одержаних результатів. Застосування напрацювань дозволить вибрати методи й інструменти виявлення загроз як ключового чинника підвищення стійкості бізнес-процесів та оптимізації ресурсів на мережеву безпеку. Це забезпечить високий рівень захисту інформаційних мереж і зменшить ризики реалізації мережевих загроз.

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

Розділ 1. ОСНОВИ МЕРЕЖЕВОЇ БЕЗПЕКИ

1.1 Безпека мережі: сутність і типи

Безпека мережі - це комплекс заходів, що забезпечують захист інформації та ресурсів мережі від різноманітних загроз. Основними типами мережевої безпеки є фізична, адміністративна та технічна.

Фізична мережева безпека

Фізична мережева безпека охоплює всі заходи, спрямовані на захист мережевого обладнання від фізичних загроз, таких як несанкціонований доступ, вандалізм або стихійні лиха.

Комплексний підхід до фізичної безпеки включає використання карток доступу, систем відеоспостереження, безперебійних джерел живлення, захисних кейсів і заходів охорони, що разом створюють надійну систему захисту мережевого обладнання [1] (Рис. 1.1).

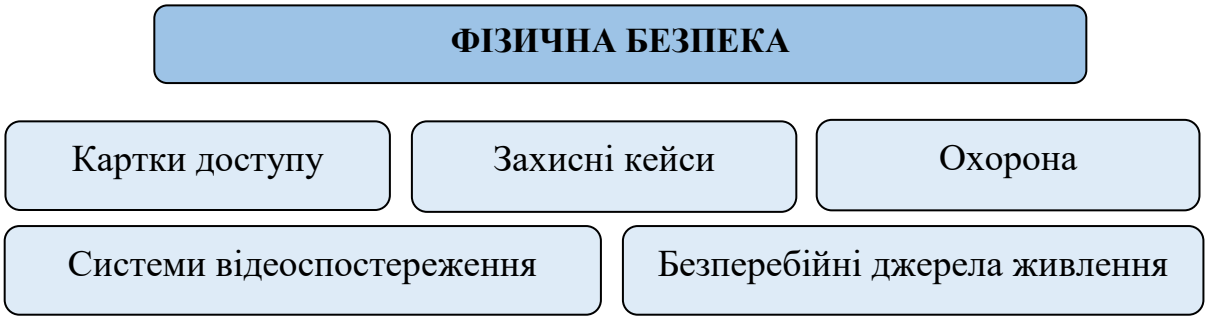

Рис. 1.1. Заходи фізичної безпеки

До цих заходів належать *використання карток доступу* для захисту приміщень, де розміщене критичне мережеве обладнання, таких як серверні кімнати або центри обробки даних. Такі приміщення можуть бути оснащені камерами спостереження, датчиками руху та системами сигналізації для виявлення та запобігання несанкціонованому доступу.

Іншим аспектом фізичної мережевої безпеки є *забезпечення надійного живлення для мережевого обладнання*. Відмови електроживлення можуть призвести до втрати даних або збоїв у роботі мережі, тому використання безперебійних джерел живлення (UPS) і генераторів є критично важливим.

Також важливо розташовувати обладнання у безпечних зонах, захищених від стихійних лих, таких як повені або землетруси, щоб значно знизити ризик фізичних загроз.

Захисні кейси та шафи для серверів забезпечують додатковий рівень захисту від фізичного пошкодження або крадіжки. Ці кейси можуть бути оснащені замками, системами вентиляції та охолодження для забезпечення оптимальних умов зберігання обладнання. Важливо також контролювати доступ до цих кейсів і регулярно перевіряти фізичну цілісність обладнання.

Охоронні заходи також можуть включати регулярні патрулювання охоронцями, особливо у великих організаціях із багатьма об'єктами мережевої інфраструктури. Такі патрулі допомагають запобігти несанкціонованому доступу та швидко реагувати на спроби проникнення. У поєднанні з електронними системами контролю доступу, такі фізичні заходи значно підвищують загальний рівень безпеки мережі.

Таким чином, фізична мережева безпека є першою лінією оборони, яка запобігає несанкціонованому доступу до критичного обладнання та забезпечує захист від фізичних загроз.

Адміністративна мережева безпека

Адміністративна мережева безпека включає в себе *створення політик, процедур і положень*, що регулюють відносини з користувачами щодо доступу та дій у мережі [2] (Рис.1.2).

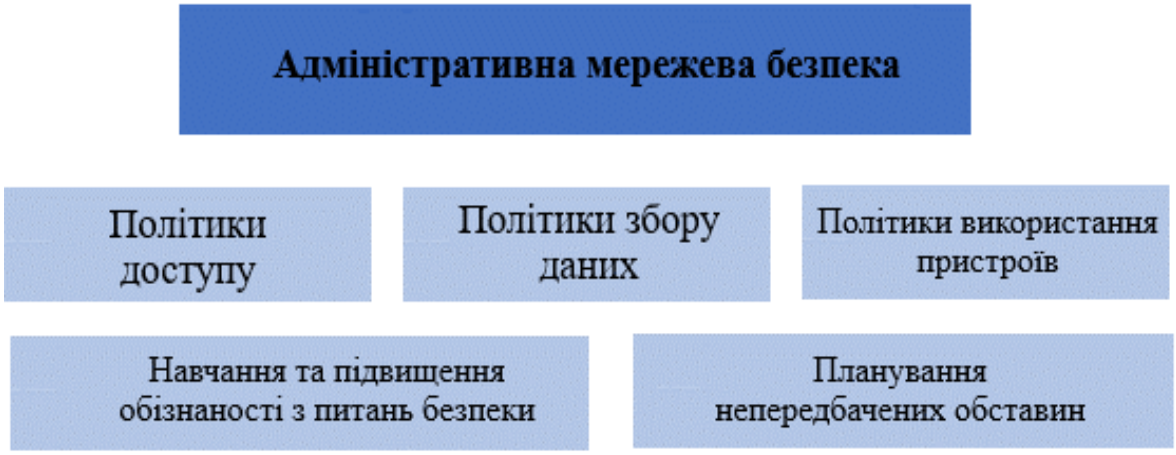

Рис. 1.2. Заходи адміністративної безпеки

Відповідно до міжнародного стандарту ISO 27002 прикладами політик у сфері мережевої безпеки є:

− контроль доступу;

− класифікація й обробка інформації;

− фізична безпека;

− безпека кінцевих користувачів (управління паролями, прийнятне використання активів, використання мобільних пристроїв і віддалена робота, обмеження інсталювання і застосування ПЗ тощо);

− резервне копіювання;

− передача інформації;

− антивірусний захист;

− криптографічний захист;

− безпека комунікацій;

− приватність і захист персональних даних;

− управління технічними вразливостями;

− зв’язки з постачальниками [3].

Наприклад, політика доступу описує доступ до ресурсів, що може бути наданий працівникам або групам людей залежно від їхньої ролі в організації та потреби у відповідної інформації. Політика управління паролями включає вимоги до складності паролів, їхнього регулярного оновлення і двофакторної аутентифікації. Вона підвищує рівень захисту, забезпечуючи додатковий шар підтвердження особистості через мобільний телефон або біометричні дані.

Адміністративна безпека також охоплює *інформування й навчання персоналу*, завдяки яким співробітники стають обізнаними про найпоширеніші загрози, такі як фішингові атаки, і навчаються використовувати правильні практики, наприклад, сильні паролі та уникнення підозрілих електронних листів. Це може бути регламентоване поводження з конфіденційною інформацією або процедури реагування на інциденти безпеки.

Також важливим елементом адміністративної безпеки є *моніторинг діяльності користувачів і виявлення підозрілих дій*. Протоколювання дій у

мережі всіх користувачів дозволяє швидко виявити аномалії та істотні загрози. Регулярний аудит цих логів допомагає швидко виявити порушення політики, що значно знижує ризик внутрішніх загроз.

Важливим елементом адміністративної безпеки мережі є процедури *реагування на інциденти*. Це можуть бути плани дій у разі виявлення зловмисних дій, витоку даних або інших інцидентів. Ці плани повинні містити чіткі ролі та відповідальності, а також процедури для відновлення мережі до нормального робочого стану [4].

Узагальнюючи, адміністративна мережева безпека встановлює корпоративні фундаменти, що дозволяють ефективно захистити мережу від широкого спектру загроз.

Технічна мережева безпека

Технічна мережева безпека охоплює використання програмного й апаратного забезпечення для захисту мережевих ресурсів (Рис. 1. 3).

Рис. 1.3. Засоби технічної безпеки

До таких засобів належать *брандмауери*, які контролюють і фільтрують мережевий трафік для запобігання несанкціонованому доступу та різного роду атакам. Брандмауери можуть бути апаратними та програмними і зазвичай розташов уються між внутрішньою мережею та Інтернетом або іншими мережами [5].

Антивірусне програмне забезпечення є ще одним ключовим компонентом технічної безпеки. Воно відповідальне за сканування файлів та трафіку на

наявність шкідливих програм, таких як віруси, трояни та шпигунське ПЗ. Регулярне оновлення антивірусних баз даних дозволяє виявити й захистити від нових загроз. Антивіруси також можуть містити додаткові функції для захисту електронної пошти та веб-браузерів від фішингових атак.

Системи виявлення та запобігання вторгнень (IDS/IPS) аналізують мережевий трафік та виявляють підозрілу активність. Ці системи можуть працювати у двох режимах: IDS-системи пасивно моніторять трафік і сповіщають про підозрілі події, тоді як IPS-системи активно блокують підозрілий трафік у реальному часі. Вони можуть виявляти як відомі, так і нові загрози за допомогою сигнатур та евристичного аналізу [6].

VPN або віртуальні приватні мережі забезпечують захищений доступ до корпоративної мережі через Інтернет. Вони створюють зашифроване з'єднання, що гарантує конфіденційність переданих даних. Це особливо важливо для віддалених користувачів, які підключаються до корпоративних ресурсів з ненадійних мереж [7].

Нарешті, технічна безпека включає *шифрування інформації* для захисту конфіденційних даних. Шифрування даних гарантує, що навіть у випадку перехоплення їх зловмисниками, вони не зможуть прочитати або використати ці дані без ключа шифрування. Це може застосовуватись як для даних, що передаються, так і для даних, що зберігаються на серверах та пристроях.

Загалом, технічна мережева безпека є важливим компонентом загальної стратегії захисту мережі, забезпечуючи захист від широкого спектру загроз.

1.2 Загрози мережевій безпеці

Загрози та методи атак на мережеву безпеку.

Загроза - це будь-яка обставина або подія, що може призвести до порушення політики безпеки інформації і/або нанесення шкоди інформаційній системі [8]. Загрози можуть бути різноманітними за природою, включаючи випадкові помилки, збої обладнання, природні лиха, а також навмисні дії

зловмисників. Вони можуть мати серйозні наслідки для організацій, включаючи фінансові втрати, втрату довіри клієнтів і пошкодження репутації.

Виділяють такі види загроз мережевій безпеці (Рис.1.4):

Рис. 1.4. Види загроз мережевій безпеці

Фізичні загрози

Фізичні загрози включають пошкодження або знищення апаратного забезпечення через стихійні лиха, пожежі або вандалізм. Такі загрози можуть бути особливо руйнівними, оскільки вони можуть призвести до втрати обладнання та даних, а також порушити роботу мережі. Наприклад, пожежа в серверній кімнаті може знищити всю інфраструктуру компанії, що вимагатиме значних ресурсів для відновлення.

Для запобігання таким загрозам важливо забезпечити надійний фізичний захист. Це включає контроль доступу до приміщень, використання захисних кейсів для обладнання, встановлення систем відеоспостереження та пожежогасіння. Крім того, регулярні перевірки стану обладнання та систем безпеки допоможуть виявити потенційні проблеми до того, як вони стануть критичними [9].

Логічні загрози

Логічні загрози включають віруси, трояни, фішинг та атаки на відмову в обслуговуванні (DoS/DDoS). Віруси та трояни є шкідливими програмами, які можуть пошкодити або знищити дані, викрасти конфіденційну інформацію або надати зловмисникам доступ до системи. Віруси можуть поширюватися через

електронні листи, завантаження з Інтернету або заражені зовнішні носії. Трояни, з іншого боку, часто маскуються під легітимні програми і можуть надавати зловмисникам віддалений доступ до комп'ютера жертви.

Фішинг спрямований на обман користувачів з метою отримання конфіденційної інформації, такої як паролі або номери кредитних карток.

Атаки на відмову в обслуговуванні (DoS/DDoS) націлені на перевантаження системи трафіком, що робить її недоступною для легітимних користувачів. Такі атаки можуть призвести до значних фінансових втрат та пошкодження репутації компанії. Для захисту від логічних загроз необхідно використовувати антивірусні програми, фаєрволи та системи виявлення вторгнень.

Соціальна інженерія

Соціальна інженерія маніпулює людьми для отримання конфіденційної інформації або доступу до системи. Це може включати фішингові листи, телефонні дзвінки або особисті зустрічі, де зловмисники видають себе за довірених осіб або організації, щоб отримати конфіденційну інформацію. Наприклад, зловмисник може відправити електронний лист, що виглядає як повідомлення від банку, і попросити користувача надати свої облікові дані.

Інші методи соціальної інженерії можуть включати використання психологічних прийомів, щоб змусити користувачів розкрити паролі або надати доступ до конфіденційних даних. Захист від соціальної інженерії вимагає проведення регулярних тренінгів для співробітників з метою підвищення їх обізнаності про такі загрози, а також впровадження політик і процедур, які мінімізують ризик несанкціонованого доступу [10].

Цільові атаки (APT)

Цільові атаки (Advanced Persistent Threats, APT) - це складні, багатоступеневі атаки, які можуть тривати протягом тривалого часу і націлені на конкретні організації або індивідууми. Такі атаки зазвичай включають кілька етапів, таких як розвідка, вторгнення, встановлення контролю і викрадення

даних. APT-атаки часто здійснюються організованими групами або державними акторами і можуть бути надзвичайно складними для виявлення та відбиття.

Захист від цільових атак вимагає багаторівневого підходу, включаючи використання передових технологій для виявлення вторгнень, моніторинг мережевого трафіку і активний захист кінцевих точок. Крім того, важливо мати плани реагування на інциденти та регулярно проводити навчання для персоналу з метою підвищення їхньої готовності до можливих атак.

Загрози з боку внутрішніх користувачів

Загрози з боку внутрішніх користувачів можуть бути навмисними або випадковими. Випадкові загрози включають помилки співробітників, такі як випадкове видалення важливих файлів або несанкціоноване розповсюдження конфіденційної інформації. Такі помилки можуть статися через недоліки в навчанні або відсутність належного контролю доступу.

Навмисні загрози можуть включати зловмисні дії співробітників, які намагаються завдати шкоди організації або викрасти інформацію. Внутрішні загрози часто важко виявити, оскільки вони можуть бути здійснені користувачами, які мають легітимний доступ до системи. Для захисту від внутрішніх загроз необхідно впроваджувати строгі політики доступу, проводити регулярний аудит систем та забезпечувати навчання персоналу з питань інформаційної безпеки [11].

Методи атак на мережеву безпеку

З кожним днем зростає кількість атак на мережеву безпеку й урізноманітнюються методи шкідливого впливу на ресурси мережі. Найбільш поширені методи атак на мережеву безпеку показані на рис. 1.5.

Віруси

Віруси не запускаються самостійно. Для їх розповсюдження та зараження мережі або комп'ютера потрібна взаємодія з користувачем. Віруси часто додаються до файлів і запускаються разом із ними, поширюючись через завантаження, електронні листи або зовнішні носії. Основні типи вірусів включають файлові віруси, завантажувальні віруси та макровіруси.

Рис. 1.5. Методи атак на мережеву безпеку

Вони можуть виконувати шкідливі дії, такі як видалення файлів, шифрування даних або викрадення конфіденційної інформації. Для захисту від вірусів необхідно використовувати антивірусні програми, регулярно оновлювати програмне забезпечення та навчати користувачів безпечним практикам роботи з електронними листами та файлами.

Шкідливе програмне забезпечення

Після зараження комп'ютера шкідливе ПЗ проникає в мережу і починає розповсюджуватися на інші підключені пристрої. Шкідливе ПЗ може включати трояни, шпигунські програми, кейлогери та інше. Трояни можуть приховуватися у вигляді легітимних програм, а кейлогери записують кожен натиск клавіші для крадіжки паролів та іншої конфіденційної інформації.

Шкідливе ПЗ може виконувати різні шкідливі дії, такі як крадіжка даних або надання віддаленого доступу до системи зловмисникам. Для захисту від шкідливого ПЗ необхідно використовувати антивірусні програми, системи виявлення вторгнень та забезпечувати регулярне оновлення ПЗ.

Хробаки

Хробаки заражають систему при запуску вразливого мережевого додатку. Вони можуть самостійно поширюватися через мережу, використовуючи вразливості в операційних системах або програмному забезпеченні. Хробаки можуть створювати копії себе і поширюватися на інші комп'ютери в мережі без потреби в дії користувача.

Вони часто використовуються для створення ботнетів або здійснення DoS-атак. Для захисту від хробаків необхідно регулярно оновлювати програмне забезпечення, використовувати фаєрволи та системи виявлення вторгнень.

Фішинг

Фішинг включає відправку електронних листів, SMS-повідомлень і інших повідомлень з посиланнями або вкладеннями, замаскованими під надійні джерела, з метою отримання конфіденційної інформації. Фішингові атаки часто використовуються для викрадення паролів, фінансових даних або іншої чутливої інформації.

Фішинг може також включати використання фальшивих вебсайтів, що імітують легітимні сайти, для обману користувачів і збору їхніх даних. Різновидом фішингу є "спірфішинг", який орієнтований на конкретних осіб або організації. Захист від фішингу включає використання антифішингових програм, навчання користувачів розпізнаванню підозрілих повідомлень та впровадження двофакторної аутентифікації [12].

Ботнет

Ботнет - це мережа приватних комп'ютерів, заражених шкідливим ПЗ і підконтрольних зловмисникам. Використовується для здійснення атак на відмову в обслуговуванні (DoS), розповсюдження спаму або виконання інших шкідливих дій.

Комп'ютери в ботнеті (так звані "зомбі") можуть виконувати команди зловмисника без відома власника. Ботнети часто використовуються для масових атак або розсилки спаму, оскільки вони дозволяють зловмисникам контролювати велику кількість комп'ютерів одночасно. Для захисту від ботнетів необхідно використовувати антивірусні програми, системи виявлення вторгнень і проводити регулярний аудит мережевої активності [13].

DoS-атака (відмова в обслуговуванні)

DoS-атака руйнує всю IT-інфраструктуру жертви, блокуючи доступ для законних користувачів. Атака досягається шляхом надмірного навантаження на сервер або мережу, що призводить до їхньої непрацездатності. DoS-атаки

можуть включати націлені дії, такі як відправлення великої кількості запитів до сервера, що перевантажує його і робить недоступним для інших користувачів.

Це може призвести до фінансових втрат та пошкодження репутації організації. Захист від DoS-атак включає використання систем захисту від DoS, моніторинг мережевого трафіку та впровадження політик обмеження доступу.

DDoS-атака (розподілена відмова в обслуговуванні)

DDoS-атака включає використання кількох скомпрометованих систем для одночасної атаки на одну систему жертви, що призводить до перевантаження і відмови в обслуговуванні. DDoS-атаки складніше запобігти через їх розподілений характер. Вони можуть використовувати ботнети для одночасної атаки з багатьох джерел, що ускладнює відслідковування джерела атаки та його блокування.Виявлення і запобігання таких атак здійснюється шляхом аналізу трафіку і активної протидії атаці. Для захисту від DDoS-атак необхідно використовувати системи захисту від DDoS, проводити регулярний моніторинг мережевого трафіку і впроваджувати політики обмеження доступу.

Атака типу «Man-in-the-Middle»

Зловмисник захоплює сеанс і краде важливі дані, якими обмінюються дві сторони, перехоплюючи їхній зв'язок. Така атака дозволяє зловмиснику контролювати, змінювати або викрадати передану інформацію. Атака "людина-посередник" може здійснюватися в мережах Wi-Fi, де зловмисник може підключитися до незахищеної мережі і перехоплювати дані, що передаються між користувачем і сервером.

Це дозволяє зловмиснику отримати доступ до конфіденційних даних або змінювати їх. Захист від таких атак включає використання шифрування даних, впровадження двофакторної аутентифікації і використання віртуальних приватних мереж (VPN) [14].

Аналіз пакетів

Це процес збору і крадіжки даних, які проходять через комп'ютерну мережу. Аналіз пакетів (або "сніффінг") може бути виконаний за допомогою спеціальних програм, які перехоплюють і аналізують мережевий трафік. Це

дозволяє виявляти незашифровані дані, що передаються через мережу, і використовувати їх для подальших атак.Використовується для виявлення вразливостей, перехоплення даних або діагностики мережевих проблем. Для захисту від аналізу пакетів необхідно використовувати шифрування даних, впроваджувати політики безпеки мережі й регулярно моніторити мережеву активність.

Підміна DNS

Компрометує мережу, пошкоджуючи сервер доменних імен (DNS), щоб повернути неправильну IP-адресу. Така атака може перенаправити користувачів на фальшиві вебсайти для викрадення даних або розповсюдження шкідливого ПЗ. Атаки на DNS можуть включати кеш-поізонування (DNS cache poisoning), що дозволяє зловмиснику змінювати записи в кеші DNS-сервера, направляючи користувачів на шкідливі сайти замість легітимних.Захист від підміни DNS включає використання захищених DNS-серверів, впровадження DNSSEC (розширення безпеки DNS) і регулярний моніторинг DNS-записів.

Підміна IP-адреси

Хакер видає себе за іншого користувача, впроваджуючи пакети в Інтернет, використовуючи фальшиву адресу джерела. Це дозволяє зловмиснику обходити механізми аутентифікації і контролю доступу, що забезпечує доступ до закритих мережевих ресурсів. Підміна IP-адреси (або "спуфінг") може використовуватися для приховування особи зловмисника або для здійснення атак, що здаються легітимними, оскільки вони виглядають як запити від надійного джерела [15].

Для захисту від підміни IP-адрес необхідно використовувати фаєрволи, системи виявлення вторгнень і впроваджувати політики контролю доступу.

Зламаний ключ

Зловмисник отримує несанкціонований доступ до мережі за допомогою зламаного захищеного ключа. Може бути використано для шифрування або підпису даних, забезпечуючи їхню цілісність і конфіденційність. Злам ключів шифрування дозволяє зловмиснику декодувати захищені дані або видавати себе за іншого користувача, що забезпечує доступ до конфіденційної інформації або

систем.Використання сильних алгоритмів шифрування і захист ключів є критично важливими для запобігання таких атак. Для захисту від зламу ключів необхідно впроваджувати політики управління ключами, регулярно оновлювати ключі шифрування та використовувати надійні методи їх зберігання.

1.3 Методи та технології запобігання і протидії мережевим загрозам

Сучасний світ значно залежить від інформаційних технологій та мережевих комунікацій, що робить питання мережевої безпеки вкрай важливим. Забезпечення безпеки інформаційних мереж вимагає комплексного підходу, який включає різноманітні методи та технології запобігання та протидії загрозам. Розглянемо основні заходи, які можуть бути впроваджені як на пристроях користувачів, так і на серверах для забезпечення високого рівня захисту [16] (Рис.1.6).

Рис. 1.6. Методи та технології запобігання і протидії мережевим загрозам

Заходи мережевої безпеки на пристроях користувачів

Контроль доступу до мережі

Система управління доступом до мережі (Network Access Control, NAC) керує правами доступу користувачів, блокує доступ до мережі пристроїв без

необхідних заходів кібербезпеки та поширює файли конфігурації на пристрої організації. NAC забезпечує, що лише авторизовані пристрої можуть підключатися до мережі, зменшуючи ризик проникнення шкідливого ПЗ або несанкціонованих користувачів. Вона також дозволяє відстежувати і контролювати всі підключення до мережі в режимі реального часу, що підвищує загальний рівень безпеки.

Контроль доступу до мережі включає кілька рівнів захисту. Наприклад, пристрої можуть бути перевірені на відповідність політикам безпеки перед тим, як їм буде надано доступ до мережі. Це може включати перевірку наявності антивірусного програмного забезпечення, актуальності оновлень операційної системи та відсутності відомих вразливостей. Крім того, NAC-системи можуть автоматично застосовувати оновлення безпеки та конфігурації для забезпечення відповідності стандартам безпеки.

Віртуальні приватні мережі (VPN)

Віртуальна приватна мережа (Virtual Private Network, VPN) переспрямовує інтернет-трафік користувача через захищений сервер, надаючи йому безпечний доступ до внутрішніх ресурсів і не дозволяючи іншим користувачам перехоплювати конфіденційні дані. Використання VPN забезпечує анонімність та захищеність під час роботи в Інтернеті, особливо при використанні загальнодоступних мереж. VPN може також захищати дані від атак типу "людина-посередник", шифруючи весь трафік між користувачем та сервером.

VPN також можуть використовувати протоколи шифрування, такі як OpenVPN, IPSec, L2TP і SSL/TLS, які забезпечують високий рівень захисту даних. Вони дозволяють створювати захищені канали зв'язку між віддаленими офісами або мобільними користувачами та центральними ресурсами компанії. Використання VPN допомагає запобігти перехопленню даних під час їх передачі через Інтернет, що є критично важливим для захисту конфіденційної інформації та підтримки цілісності даних [17].

Захист від шкідливих програм

Антивіруси та інші програми для захисту від шкідливого програмного забезпечення допомагають запобігати поширенню заражених об'єктів по всій мережі. Антивірусні програми дозволяють ідентифікувати зараження, сповіщати про це службу безпеки та поміщати файли на карантин, доки не буде знайдено відповідне рішення. Антивірусні програми можуть також забезпечувати активний захист, перевіряючи всі файли та програми в режимі реального часу на наявність потенційних загроз.

Для ефективного захисту від шкідливих програм важливо використовувати багаторівневий підхід. Це включає регулярні оновлення антивірусних баз даних, використання технологій проактивного захисту, таких як поведінковий аналіз і машинне навчання, а також впровадження політик безпеки, які обмежують можливості користувачів встановлювати та запускати неперевірене програмне забезпечення. Крім того, важливо навчати користувачів розпізнавати ознаки шкідливих програм та реагувати на них.

Багатофакторна автентифікація

Багатофакторна автентифікація (Multi-Factor Authentication, MFA) вимагає від користувачів виконувати додаткові кроки для підтвердження їхньої особи в мережі. MFA може перешкоджати зловмисникам завдавати шкоди за допомогою пароля користувача високого рівня. Це може включати додатковий код, відправлений на мобільний телефон, або біометричні дані, такі як відбиток пальця. Використання MFA значно підвищує рівень безпеки, оскільки навіть у разі компрометації пароля доступ до системи все одно буде заблокований без другого фактора автентифікації.

MFA знижує ризик несанкціонованого доступу до критичних систем і даних, навіть якщо один з факторів автентифікації був скомпрометований. Впровадження MFA може включати використання одноразових паролів (OTP), апаратних токенів, біометричних методів (відбитки пальців, розпізнавання обличчя) та інших методів для підвищення безпеки. Це значно ускладнює життя зловмисникам, оскільки для отримання доступу необхідно пройти через кілька рівнів захисту [18].

Заходи мережевої безпеки на серверах

Брандмауери

Брандмауер блокує спроби доступу до мережі несанкціонованих користувачів або пристроїв. Брандмауери варіюються від простих пакетних фільтрів до найсучаснішого програмного забезпечення зі складним ШІ для динамічного аналізу даних. Вони є першою лінією захисту від зовнішніх атак, контролюючи вхідний і вихідний трафік на основі встановлених правил. Сучасні брандмауери також можуть інтегруватися з іншими системами безпеки, такими як системи виявлення вторгнень (IDS), для забезпечення комплексного захисту.

Брандмауери можуть бути як апаратними, так і програмними, кожен з яких має свої переваги. Апаратні брандмауери забезпечують високу продуктивність і безпеку, оскільки вони працюють незалежно від операційної системи сервера. Програмні брандмауери, з іншого боку, можуть бути налаштовані для більш гнучкого управління трафіком і інтеграції з іншими програмними рішеннями безпеки. Важливим аспектом є також впровадження політик безпеки, що регулюють правила роботи брандмауерів та їх оновлення.

Системи виявлення вторгнень (IDS)

Система виявлення вторгнень (Intrusion Detection System, IDS) постійно відстежує дії в мережі на предмет відхилень від нормальної поведінки. IDS часто поєднується із системами запобігання вторгненням (IPS), щоб автоматично реагувати на порушення. Вони можуть виявляти підозрілі активності, такі як несанкціоновані спроби доступу або атаки типу "людина-посередник". IDS може аналізувати мережевий трафік у реальному часі, ідентифікуючи потенційні загрози та сповіщаючи адміністраторів про необхідність вжиття заходів.

IDS-системи можуть використовувати сигнатури відомих атак або аномалії в поведінці мережі для виявлення потенційних загроз. Це дозволяє швидко реагувати на нові типи атак, які можуть не бути виявлені традиційними методами. Крім того, IDS можуть бути інтегровані з іншими системами безпеки, такими як брандмауери та системи управління інформацією та подіями безпеки (SIEM), для покращення загального рівня безпеки мережі.

Засоби запобігання втраті даних (DLP)

Замість того, щоб блокувати доступ зловмисників, засоби щодо запобігання втраті даних (Data Leakage Prevention, DLP) перешкоджають витоку конфіденційної інформації з мережі. Наприклад, DLP може передбачати вимогу шифрування файлів, що зберігаються в хмарі. Ці системи допомагають захистити інтелектуальну власність і конфіденційну інформацію від несанкціонованого розголошення. DLP-системи можуть також виявляти та блокувати передачу чутливої інформації по незахищених каналах.

DLP-рішення можуть бути як апаратними, так і програмними, і вони інтегруються в різні точки мережі для забезпечення комплексного захисту. Вони здатні виявляти і блокувати спроби передачі конфіденційних даних за межі організації через електронну пошту, веб-додатки, знімні носії або інші канали. Крім того, DLP-системи можуть автоматично застосовувати політики безпеки, що регулюють обробку та зберігання конфіденційної інформації, забезпечуючи відповідність нормативним вимогам і внутрішнім стандартам безпеки [19].

Захищені вебшлюзи

Захищені вебшлюзи поєднують у собі аспекти брандмауерів, інструменти фільтрації URL-адрес і заходи контролю програм для запобігання доступу хакерів до мережі або відвідування небезпечних сайтів інсайдерами. Вони забезпечують комплексний підхід до захисту вебтрафіку, фільтруючи небажаний контент і блокуючи підозрілі сайти. Захищені вебшлюзи можуть також запобігати завантаженню шкідливого програмного забезпечення та контролювати доступ користувачів до інтернет-ресурсів.

Сучасні вебшлюзи можуть використовувати технології машинного навчання для аналізу вебтрафіку та виявлення нових загроз у режимі реального часу. Вони також можуть інтегруватися з іншими системами безпеки, такими як DLP та антивірусні програми, для забезпечення багаторівневого захисту. Захищені вебшлюзи допомагають знижувати ризики, пов'язані з вебзагрозами, та забезпечують безпечний доступ до Інтернету для співробітників, мінімізуючи ймовірність компрометації внутрішніх систем через шкідливі вебсайти.

Висновки до розділу 1

Дослідження показало, що мережева безпека є комплексом заходів, що забезпечують захист інформації та ресурсів мережі від різноманітних загроз. Основними типами мережевої безпеки є фізична, адміністративна та технічна.

Фізична мережева безпека охоплює всі заходи, спрямовані на захист мережевого обладнання від фізичних загроз, таких як несанкціонований доступ, вандалізм або стихійні лиха. Адміністративна безпека мережі включає створення політик, процедур і положень, що регулюють відносини з користувачами щодо доступу та дій у мережі. Технічна мережева безпека передбачає використання програмного й апаратного забезпечення для захисту мережевих ресурсів.

Встановлено, що загроза - це будь-яка обставина або подія, що може призвести до порушення політики безпеки інформації і/або нанесення шкоди інформаційній системі. Загрози можуть мати серйозні наслідки для організацій, включаючи фінансові втрати, втрату довіри клієнтів і пошкодження репутації.

Виділяють такі види загроз мережевій безпеці: фізичні, логічні, загрози соціальної інженерії, цільові атаки (APT), внутрішні загрози. Методи атак на мережеву безпеку охоплюють шкідливе ПЗ, фішинг, ботнети, DoS /DDoS-атаки, атака типу «Man-in-the-Middle», аналіз пакетів, підміна DNS і IP-адреси тощо.

Методи та технології запобігання і протидії мережевим загрозам поділяють на заходи мережевої безпеки на пристроях користувачів і серверах. Основними заходами мережевої безпеки на пристроях користувачів є контроль доступу до мережі (NAC), віртуальні приватні мережі (VPN), захист від шкідливих програм, багатофакторна автентифікація. Заходи мережевої безпеки на серверах охоплюють використання міжмережевих екранів, систем виявлення вторгнень (IDS), засобів запобігання втраті даних (DLP), захищених вебшлюзів.

Розділ 2. ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ЗАГРОЗ БЕЗПЕЦІ МЕРЕЖІ

2.1 Види технологій виявлення загроз мережевій безпеці

В еру стрімкого технологічного розвитку, цифровізації та всеохоплюючого підключення до Інтернету питання мережевої безпеки набувають ключовими значення для прогресу в різних сферах. Сучасні організації повинні впроваджувати проактивний підхід до забезпечення безпеки мережі, який спрямований на запобігання новим загрозам і викликам кібербезпеки. Ці завдання виконують технології виявлення загроз мережевій безпеці, основні з яких показані на рисунку 2.1.

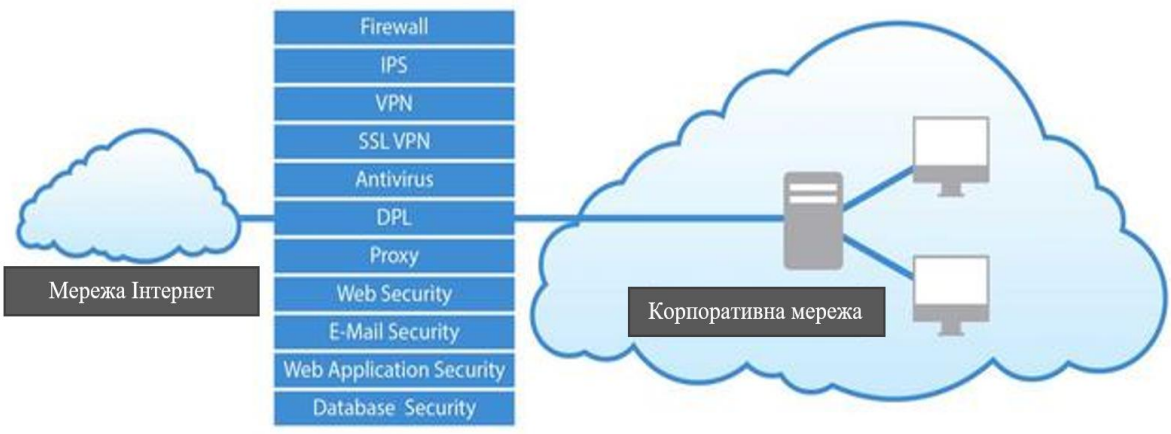

Рис. 2.1. Технології виявлення загроз мережі

Коротко розглянемо принципи їх функціонування і призначення.

Брандмауери (Firewalls)

Брандмауери контролюють потік мережевого трафіку між різними сегментами мережі, дозволяючи або блокуючи його на основі встановлених правил безпеки. Вони можуть бути як апаратними, так і програмними, та часто використовуються для захисту периметра мережі від зовнішніх загроз. Сучасні брандмауери підтримують розширені функції, такі як глибокий аналіз пакетів (DPI), що дозволяє виявляти шкідливий трафік на рівні додатків. Вони також можуть інтегруватися з іншими системами безпеки для забезпечення комплексного захисту.

Принцип функціонування брандмауера показано на рис. 2.2.

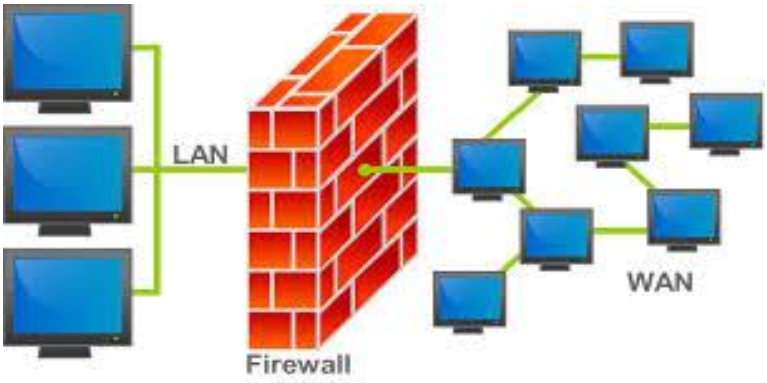

Рис. 2.2. Принцип роботи брандмауера

Системи виявлення вторгнень (Intrusion Detection System, IDS)

Система виявлення/запобігання вторгненням – це програмний або апаратний засіб для виявлення випадків несанкціонованого доступу в інформаційну або комунікаційну систему або несанкціонованого управління такими системами переважно через Інтернет. Системи виявлення вторгнень поділяють на мережеві й хостові.

Мережеві IDS (Network Intrusion Detection System, NIDS) аналізують мережевий трафік у реальному часі на предмет відомих атак або аномалій, використовуючи бази сигнатур та евристичні методи. Вони розташовані на стратегічних точках у мережі, таких як шлюзи або вузли периметра, і генерують оповіщення, що дозволяє адміністраторам швидко реагувати на потенційні загрози. NIDS можуть бути інтегровані з іншими системами безпеки, такими як SIEM, для забезпечення глибшого аналізу інцидентів.

Хостові IDS (Host Intrusion Detection System, HIDS) встановлюються на окремих пристроях, моніторять системні журнали, файли та процеси на предмет аномалій. Вони можуть виявляти зміни в критичних файлах, несанкціоновані спроби доступу та інші види підозрілої активності. HIDS часто використовуються для захисту критичних серверів і забезпечують додатковий рівень безпеки, особливо у поєднанні з іншими засобами захисту [20].

Системи запобігання вторгненням (IPS)

Системи запобігання вторгненням теж поділяють на мережеві й хостові.

Мережеві IPS (NIPS) активно втручаються у мережевий трафік для блокування шкідливої активності, використовуючи ті ж самі методи аналізу, що й NIDS. Вони можуть автоматично блокувати підозрілий трафік, відключати з'єднання або ізолювати скомпрометовані сегменти мережі. NIPS часто використовуються у поєднанні з брандмауерами для забезпечення більш глибокого аналізу та захисту на рівні додатків, що дозволяє запобігти атакам у реальному часі.

Хостові IPS (HIPS): HIPS забезпечують захист окремих пристроїв, блокуючи підозрілі процеси та дії у режимі реального часу. Вони можуть виявляти та зупиняти атаки, такі як буферні переповнення, спроби експлуатації вразливостей або зміни у критичних системних файлах. HIPS ефективні для захисту від цільових атак на окремі пристрої чи додатки [21].

Принцип дії IDS/IPS показано на рис. 2.3.

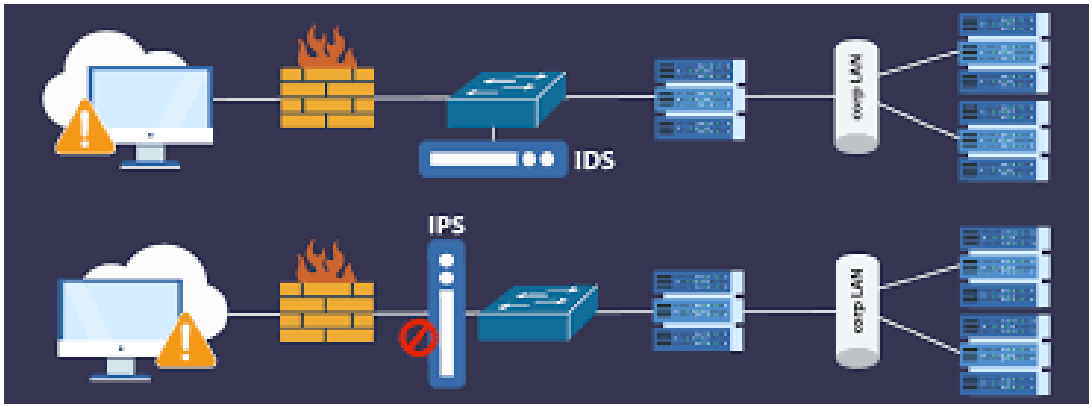

Рис. 2.3. Системи виявлення/запобігання вторгненням IDS/IPS

Віртуальні приватні мережі (VPN)

VPN забезпечують безпечне з'єднання між користувачами та корпоративною мережею через Інтернет. Вони використовують методи шифрування для захисту даних, що передаються, та забезпечують анонімність користувачів. VPN є важливими для забезпечення безпеки віддаленого доступу до корпоративних ресурсів, особливо в умовах збільшення кількості віддалених працівників. Схема функціонування віртуальних приватних мереж представлена на рис. 2.4.

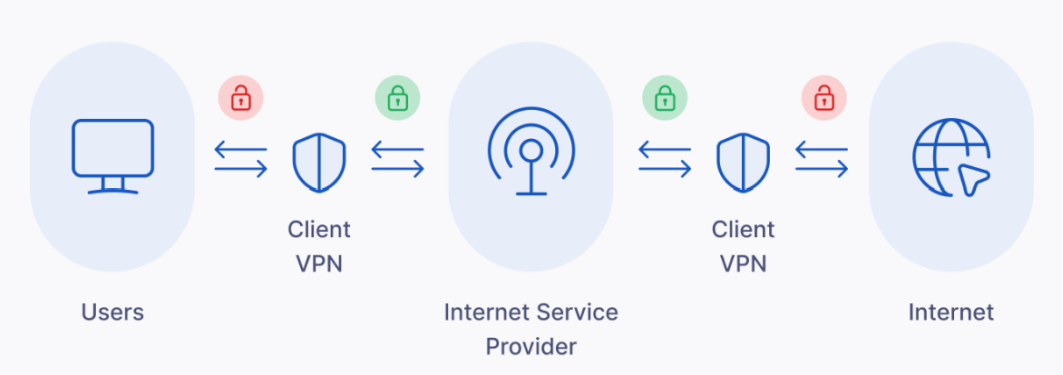

Рис. 2.4. Схема функціонування VPN

Використання VPN дозволяє забезпечити конфіденційність і цілісність даних, що передаються між віддаленими користувачами і корпоративною мережею.

Антивірусні програми

Антивірусні програми сканують системи на наявність відомих шкідливих програм, використовуючи бази сигнатур. Вони також можуть застосовувати евристичний аналіз для виявлення нових загроз, які не були раніше ідентифіковані. Багато антивірусів включають функціонал поведінкового аналізу, який дозволяє моніторити активність програм у режимі реального часу та виявляти підозрілі дії, такі як спроби зміни системних файлів або запуск несанкціонованих процесів. Це забезпечує багаторівневий захист від різних типів шкідливого програмного забезпечення.

Системи захисту від витоку даних (Data Loss Prevention, DLP)

DLP-системи забезпечують захист конфіденційних даних від несанкціонованого доступу та витоку. Вони аналізують потік даних у мережі та на кінцевих пристроях для виявлення та блокування передачі конфіденційної інформації. DLP-системи можуть використовувати різні методи, такі як шифрування, контроль доступу та моніторинг активності користувачів, для забезпечення безпеки даних. Це дозволяє запобігти витоку критичної інформації, що може призвести до серйозних фінансових та репутаційних втрат.

Системи захисту веб-доступу (Web Security Systems)

Ці системи забезпечують захист користувачів під час роботи в Інтернеті, блокуючи доступ до шкідливих сайтів та захищаючи від веб-загроз, таких як

фішинг, шкідливі скрипти та експлойти. Вони можуть використовувати методи URL-фільтрації, аналізу контенту та поведінкового аналізу для забезпечення безпеки веб-доступу. Це дозволяє зменшити ризик компрометації через веб-додатки та забезпечити захист під час перегляду Інтернету.

Системи аналізу поведінки (Behavioral Analysis Systems)

Системи аналізу поведінки використовують методи машинного навчання для створення моделей нормальної активності користувачів та пристроїв. Вони аналізують історичні дані для встановлення базових рівнів поведінки та виявляють аномалії, які можуть свідчити про загрози. Наприклад, якщо користувач, який зазвичай працює в одному часовому поясі, раптово починає здійснювати активність з іншого регіону, це може бути ознакою компрометації акаунту. Такі системи дозволяють виявляти складні та нові загрози, які важко виявити іншими методами [22].

На рис. 2.5 показано принцип дії засобів поведінкового аналізу в мережі.

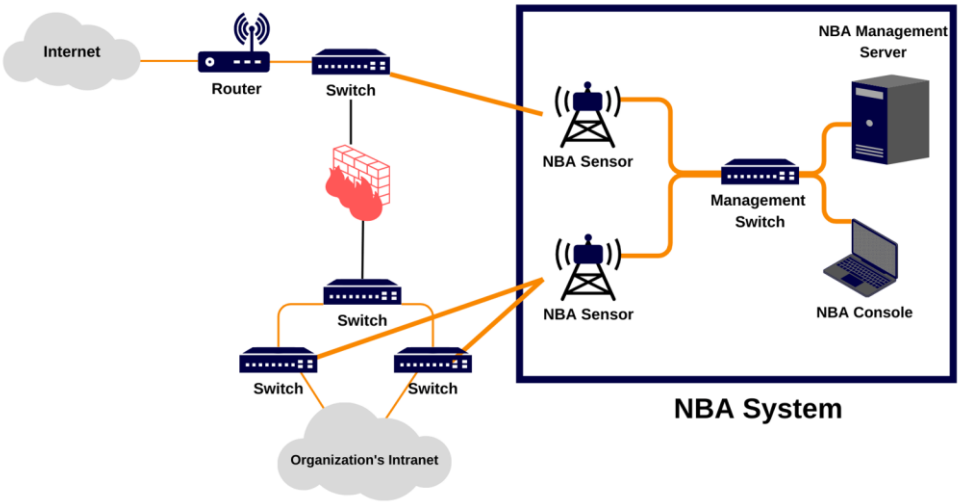

Рис. 2.5. Принцип дії засобів поведінкового аналізу в мережі

Системи захисту електронної пошти (Email Security Systems)

Ці системи забезпечують захист від фішингових атак, шкідливих вкладень та інших загроз, що передаються електронною поштою. Вони використовують методи фільтрації контенту, аналізу загроз та аутентифікації відправників для забезпечення безпеки електронної кореспонденції. Такі системи можуть також

використовувати пісочниці для аналізу підозрілих вкладень перед їх відкриттям користувачами. Це дозволяє запобігти компрометації систем через електронну пошту, яка є однією з основних цілей для зловмисників.

Пісочниці (Sandboxing)

Пісочниці забезпечують безпечне середовище для запуску підозрілих файлів і програм. У такому ізольованому середовищі детально аналізують їхню поведінку, включаючи спроби змінити системні файли, мережеву активність або інші підозрілі дії. Це дозволяє виявляти нові та складні загрози, які можуть бути не виявлені традиційними методами. Пісочниці є особливо корисними для аналізу шкідливих програм, що розповсюджуються через електронну пошту або завантажуються з Інтернету, перед їх запуском у реальних системах.

Розширене виявлення та реагування (EDR)

Однією з функцій EDR-систем, які забезпечують глибокий аналіз і моніторинг кінцевих пристроїв у режимі реального часу, є збирання даних про всі дії, що виконуються на пристроях. Ці дані використовують для виявлення аномалій та потенційних загроз. EDR-системи можуть автоматично ізолювати заражені пристрої, видаляти шкідливі програми та відновлювати системи до безпечного стану. Вони також надають інструменти для детального аналізу інцидентів та збору доказів, що є важливим для реагування на інциденти та розслідування [23].

Аналіз трафіку та протоколів (Network Traffic Analysis, NTA)

NTA-системи аналізують мережевий трафік на предмет виявлення аномалій та загроз. Вони використовують методи глибокого аналізу пакетів (DPI) для детального дослідження вмісту мережевого трафіку. Це дозволяє виявляти підозрілу активність, таку як сканування портів, несанкціонований доступ або передача конфіденційних даних. NTA-системи також можуть використовувати методи машинного навчання для створення моделей нормальної поведінки та виявлення відхилень від неї. Це дозволяє їм ефективно виявляти складні атаки, які можуть залишатися непоміченими іншими засобами захисту [24].

Системи обману (Deception Technology)

Системи обману використовують хибні цілі (honeypots) для виявлення і знешкодження атак на корпоративні мережі. Вони створюють віртуальні середовища, які імітують реальні системи та дані, приваблюючи зловмисників. Коли атака здійснюється на одну з таких хибних цілей, система реєструє всі дії хакера, що дозволяє виявити методи й інструменти, які він використовує. Це також допомагає відволікти зловмисників від реальних систем і зменшити ризик успішної атаки. Крім того, такі системи надають важливу інформацію про нові методи атак, що допомагає покращити загальну стратегію безпеки організації [25].

Системи інформаційної безпеки та управління подіями (SIEM)

SIEM-системи збирають дані з різних джерел, таких як журнали подій, мережеві пристрої, антивірусні програми та інші засоби безпеки, і корелюють їх для виявлення складних загроз. Вони забезпечують централізовану панель для моніторингу інцидентів безпеки, що дозволяє адміністраторам швидко реагувати на загрози та мінімізувати ризики. SIEM-системи можуть також використовувати методи машинного навчання для покращення точності виявлення загроз, що робить їх ефективними для виявлення багатоступеневих атак та кореляції різних типів даних [26].

Технології штучного інтелекту та машинного навчання (AI/ML)

AI/ML-технології використовуються для виявлення складних і нових загроз шляхом аналізу великих обсягів даних і побудови моделей для прогнозування. Вони можуть аналізувати мережевий трафік, журнали подій, поведінку користувачів та інші дані для виявлення аномалій і потенційних загроз. Методи машинного навчання дозволяють створювати самонавчальні системи, які постійно вдосконалюються та адаптуються до нових видів атак. Це робить їх надзвичайно ефективними для виявлення нових і раніше невідомих загроз, забезпечуючи проактивний захист мереж [27].

2.2 Системи виявлення та запобігання вторгненням (IDS/IPS)

Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) є важливими складовими превентивного підходу сучасної мережевої безпеки. Вони дозволяють організаціям виявляти та запобігати шкідливим діям у мережах і на пристроях. Розглянемо ці системи детальніше.

На рис. 2.6 показано схему функціонування IDS/IPS.

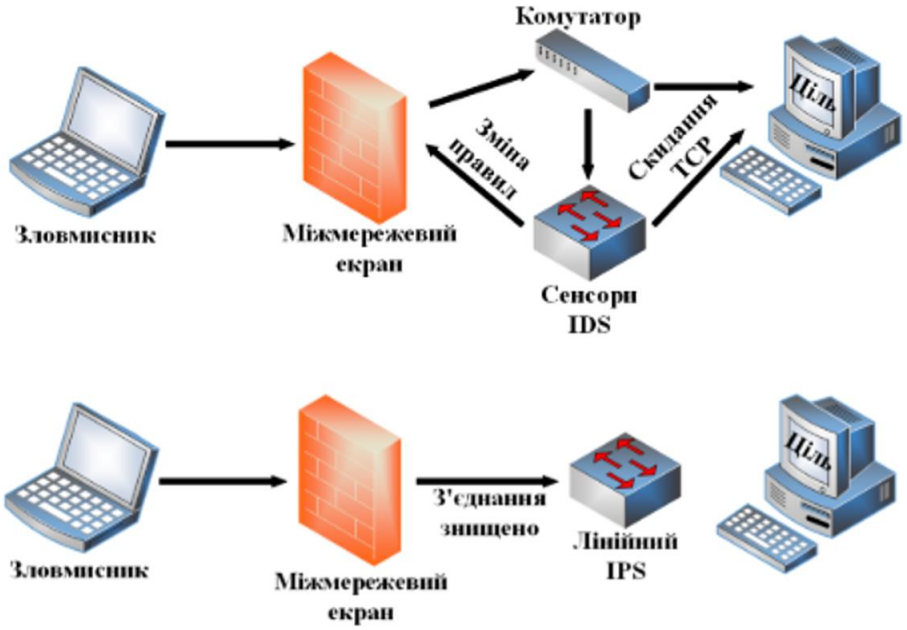

Рис. 2.6. Системи виявлення та запобігання вторгнень (IDS/IPS)

Основні компоненти IDS/IPS

Сигнатурний аналіз використовує базу відомих сигнатур для виявлення загроз. Сигнатури - це унікальні шаблони, які відповідають відомим атакам, таким як віруси, трояни або експлойти. Сигнатурний аналіз дозволяє швидко і точно виявляти відомі загрози. Однак він менш ефективний проти нових або змінених загроз, які не мають відомих сигнатур.

Аналіз на основі аномалій передбачає виявлення аномальної поведінки шляхом порівняння з базовими профілями нормальної активності. Система навчена розпізнавати нормальний трафік і виявляти відхилення від цієї норми. Цей метод дозволяє виявляти нові, раніше невідомі загрози, але може спричинити велику кількість фальшивих спрацьовувань.

Глибокий аналіз пакетів (DPI) полягає в аналізі вмісту мережевих пакетів для виявлення шкідливої активності на рівні додатків. DPI дозволяє аналізувати не тільки заголовки пакетів, але й їхній вміст. DPI є ефективним для виявлення складних атак, таких як експлойти у веб-додатках, але потребує значних обчислювальних ресурсів [28].

Як відзначалося вище, виділяють мережеві та хостові системи IDS/IPS.

Мережеві IDS розташовуються на стратегічних точках мережі, таких як шлюзи або маршрутизатори, і аналізують весь мережевий трафік у реальному часі. NIDS є ефективними для виявлення атак на мережевому рівні, таких як сканування портів або атаки типу "відмова у обслуговуванні" (DoS). Хостові IDS встановлюються на окремих пристроях, таких як сервери чи робочі станції. HIDS аналізують системні журнали, файли та процеси для виявлення підозрілої активності. HIDS забезпечують захист на рівні хоста і є ефективними для виявлення інсайдерських загроз або цільових атак на конкретні системи.

Мережеві IPS (NIPS) розміщуються по периметру мережі або у стратегічних точках і активно блокують шкідливий трафік у реальному часі. NIPS є ефективними для запобігання атакам, дозволяючи автоматично блокувати підозрілий трафік або ізолювати скомпрометовані сегменти мережі. Хостові IPS (HIPS) встановлюються на окремих пристроях і активно запобігають шкідливій активності на рівні хоста, блокуючи підозрілі процеси та дії. HIPS забезпечують додатковий рівень захисту для критичних систем, блокуючи атаки на рівні операційної системи та додатків.

Додаткові функції та можливості IDS/IPS охоплюють:

Контекстний аналіз використовується IDS/IPS для врахування додаткової інформації про мережу, такої як типи пристроїв, протоколи й характер трафіку. Це допомагає знизити число хибних спрацювань і підвищити точність виявлення.

Інтеграція з іншими системами безпеки - IDS/IPS можуть інтегруватися з SIEM-системами для централізованого управління та кореляції подій безпеки. Це дозволяє отримувати більш повну картину про інциденти безпеки та швидше

реагувати на загрози. Інтеграція з брандмауерами й антивірусами забезпечує додатковий рівень захисту, поєднуючи різні методи виявлення і блокування загроз.

Автоматизація та оркестрація: Сучасні IDS/IPS використовують автоматизацію для виконання рутинних завдань та швидкої реакції на інциденти. Наприклад, вони можуть автоматично блокувати IP-адреси, відомі як шкідливі, або застосовувати оновлення політик безпеки. Оркестрація дозволяє інтегрувати IDS/IPS з іншими інструментами кібербезпеки, такими як платформи SOAR (Security Orchestration, Automation, and Response), для комплексного управління інцидентами.

Машинне навчання та штучний інтелект використовуються для покращення точності виявлення загроз. AI/ML алгоритми можуть аналізувати великі обсяги даних та виявляти складні шаблони загроз, які важко виявити традиційними методами. Машинне навчання також допомагає знижувати кількість фальшивих спрацьовувань, вдосконалюючи моделі виявлення на основі нових даних.

Хмарні рішення: Перехід до хмарних IDS/IPS дозволяє забезпечити гнучкість та масштабованість, необхідну для сучасних динамічних мереж. Хмарні рішення можуть бути швидко розгорнуті та оновлені, що забезпечує постійний захист від нових загроз. Хмарні IDS/IPS можуть використовуватися для захисту хмарних середовищ та інфраструктури, забезпечуючи безпеку даних та додатків у хмарі.

Виявлення та запобігання просунутим постійним загрозам (*APT, Advanced Persistent Threats)* - IDS/IPS можуть бути налаштовані для виявлення ознак (APT), які часто включають багатоступеневі та тривалі атаки. Це досягається за рахунок детального аналізу поведінки та використання методів кореляції подій. Виявлення APT включає моніторинг аномальних дій, таких як тривалі та повторювані спроби доступу до конфіденційних даних або мережевих ресурсів [29].

Дослідження показало, що IDS/IPS притаманні як переваги, так і недоліки.

Основними перевагами IDS/IPS є:

Раннє виявлення загроз - IDS/IPS-системи дозволяють виявляти загрози на ранній стадії, до того як вони можуть завдати значної шкоди, забезпечуючи проактивний підхід до мережевої безпеки, і запобігати інцидентам, а не реагувати на них постфактум. Раннє виявлення дозволяє знизити ризик успішних атак і мінімізувати потенційні збитки.

Активна відповідь на загрози (IPS) - IPS-системи не тільки виявляють загрози, але й активно втручаються у мережевий трафік, блокуючи шкідливу активність у режимі реального часу. Це дозволяє запобігати атакам у момент їхнього виявлення. Активна відповідь передбачає блокування підозрілого трафіку, відключення з'єднань або ізоляцію скомпрометованих сегментів мережі.

Моніторинг мережевого трафіку - IDS/IPS-системи забезпечують постійний моніторинг мережевого трафіку, виявляючи аномалії та підозрілу активність. Це дозволяє підтримувати високий рівень безпеки мережі та швидко реагувати на потенційні загрози. Моніторинг трафіку включає аналіз пакетів даних, виявлення аномалій у трафіку й аналіз поведінки користувачів.

Забезпечення нормативної відповідності - IDS/IPS-системи допомагають організаціям відповідати вимогам нормативних актів і стандартів, таких як GDPR, PCI DSS та HIPAA. Вони забезпечують необхідний рівень контролю та звітності, що дозволяє демонструвати відповідність вимогам регуляторів. Впровадження IDS/IPS-систем може бути обов'язковим вимогою для деяких галузей або контрактів.

Інтеграція з іншими системами безпеки - IDS/IPS-системи можуть бути інтегровані з іншими засобами кібербезпеки, такими як SIEM, антивірусні програми і фаєрволи, забезпечуючи комплексний підхід до захисту систем і мереж. Інтеграція дозволяє об'єднувати дані з різних джерел, покращуючи аналіз та кореляцію подій.

Серед недоліків IDS/IPS виділяють:

Фальшиві спрацьовування - IDS/IPS-системи нерідко генерують велику кількість хибних спрацювань, що може вимагати додаткових зусиль для їх перевірки та фільтрації, а отже, призводити до втрати часу та ресурсів. Хибні

спрацювання знижують ефективність системи та відволікають фахівців з безпеки від реальних загроз.

Складність налаштування й управління - впровадження та налаштування IDS/IPS-систем (налаштування правил виявлення, аналізу трафіку та реагування на інциденти) є досить складним завданням, що вимагає високого рівня експертизи і значних ресурсів. Підтримка й оновлення системи також можуть вимагати значних зусиль і ресурсів.

Високі потреби в ресурсах - IDS/IPS-системи часто потребують значних обчислювальних ресурсів для аналізу мережевого трафіку в режимі реального часу, зокрема високопродуктивного апаратного забезпечення і пропускної здатності мережі. Високі вимоги до ресурсів можуть бути проблемою для малих і середніх компаній з обмеженими можливостями.

Обмежена ефективність проти нових загроз - IDS/IPS-системи, які використовують сигнатурний аналіз, можуть бути менш ефективними проти нових або невідомих загроз, які не мають відомих сигнатур. Таким чином обмежується їхня здатність виявляти нові види атак. Для покращення ефективності проти нових загроз необхідно використовувати поведінковий аналіз і методи машинного навчання.

Потенційний вплив на продуктивність мережі - впровадження IPS-систем може впливати на продуктивність мережі, оскільки вони втручаються у мережевий трафік для блокування шкідливої активності. Це може призводити до затримок або зниження пропускної здатності мережі. Для зменшення впливу на продуктивність необхідно ретельно налаштовувати IPS-систему та оптимізувати її роботу [30].

Отже, системи виявлення та запобігання вторгненням (IDS/IPS) є важливими інструментами для забезпечення безпеки мережі. Вони мають значні переваги, такі як раннє виявлення загроз, активна відповідь на загрози, моніторинг мережевого трафіку та підтримка нормативної відповідності. Однак, вони також мають певні недоліки, такі як фальшиві спрацьовування, складність налаштування та управління, високі вимоги до ресурсів, обмежена ефективність

проти нових загроз та потенційний вплив на продуктивність мережі. Для максимальної ефективності IDS/IPS-систем необхідно враховувати ці недоліки та впроваджувати додаткові засоби безпеки, такі як поведінковий аналіз і машинне навчання.

2.3 Технології розширеного виявлення та реагування (EDR)

Розширене виявлення та реагування (Endpoint Detection and Response, EDR) є передовою технологією, яка забезпечує глибокий аналіз активності на кінцевих пристроях (endpoints), дозволяє виявляти і реагувати на складні загрози у реальному часі. EDR-системи є критичним компонентом сучасної стратегії мережевої безпеки, оскільки вони забезпечують проактивний підхід до виявлення та реагування на загрози. Принцип роботи EDR показано на рис. 2.7.

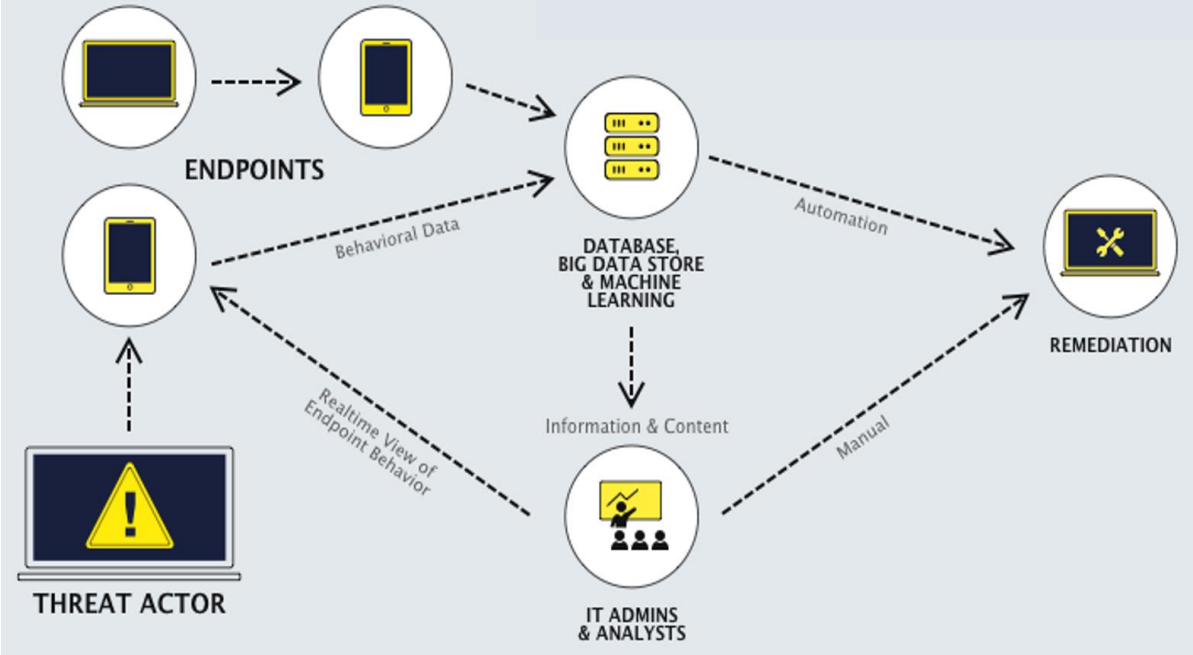

Рис. 2.7. Принцип роботи EDR

Основними компонентами EDR-систем, які забезпечують виявлення загроз мережевій безпеці, є:

Моніторинг активності на кінцевих пристроях, у рамках яких EDR-системи постійно збирають та аналізують дані про активність на кінцевих пристроях, включаючи процеси, мережевий трафік, зміни у файловій системі та

інші важливі події. Безперервний моніторинг дозволяє отримувати повну картину про те, що відбувається на пристрої (запущені процеси, створення або видалення файлів, підключення до мережі, зміни у реєстрі Windows тощо) і вчасно виявляти підозрілу активність. Наприклад, збір інформації про всі.

Виявлення загроз - EDR-системи використовують різні методи для виявлення загроз, включаючи кілька видів аналізу (сигнатурний, евристичний, поведінковий) і методи машинного навчання. Це забезпечує можливість виявлення як відомих, так і нових загроз, включаючи складні атаки, які важко виявити іншими засобами. Наприклад, виявлення шкідливого ПЗ на основі відомих сигнатур або визначення підозрілої активності на основі поведінкових аномалій.

Крім зазначених функцій EDR-системи забезпечують *реагування і розслідування інцидентів.*

Основними функціями EDR є:

Збір даних у реальному часі. EDR-системи збирають дані про активність на кінцевих пристроях у режимі реального часу, включаючи запущені процеси, мережеві з'єднання, зміни у файловій системі, доступ до реєстру, логіни та логаути користувачів тощо. Це забезпечує постійний моніторинг та виявлення підозрілої активності.

Аналіз та кореляція. EDR-системи аналізують зібрані дані для виявлення аномалій та підозрілої активності. Вони використовують методи кореляції для виявлення зв'язків між подіями та виявлення складних атак. Методи машинного навчання допомагають підвищити точність аналізу та знизити кількість фальшивих спрацьовувань [31].

Крім зазначених функцій EDR-системи здійснюють автоматичне реагування на виявлені загрози; цифрову криміналістику й розслідування інцидентів; звітування й аналітику.

EDR-системи мають низку переваг, серед яких забезпечення проактивного підходу шляхом виявлення й нейтралізації загроз на ранній стадії, до того як вони можуть завдати значної шкоди; швидка реакція на інциденти; глибокий

аналіз та розслідування, що дозволяє виявляти причини та наслідки атак; невисока кількість хибних спрацювань завдяки використанню методів машинного навчання і поведінкового аналізу; масштабованість та гнучкість, що дозволяє забезпечити високий рівень захисту незалежно від розміру організації та кількості пристроїв.

До недоліків систем EDR відносять: *складність в*провадження та управління EDR-системами, що вимагає високого рівня експертизи і значних ресурсів; висока в*артість* впровадження й супроводу, особливо у великих організаціях з великою кількістю кінцевих пристроїв; п*роблеми з конфіденційністю, оскільки з*бір та аналіз великих обсягів даних про активність користувачів може вимагати дотримання нормативних вимог щодо забезпечення конфіденційності таких даних.

Розвитку сучасних систем EDR характерні такі тенденції:

Інтеграція з іншими засобами кібербезпеки - EDR-системи часто інтегруються з іншими засобами безпеки, такими як SIEM, SOAR і антивірусні програми, для забезпечення комплексного захисту. Інтеграція дозволяє мати більш повну картину про загрози й події безпеки, швидше на них реагувати.

Використання штучного інтелекту та машинного навчання - AI/ML технології дозволяють покращити точність виявлення загроз, автоматизувати рутинні завдання та знижувати кількість фальшивих спрацювань. ML допомагає створювати більш точні моделі поведінки й виявляти складні атаки, які важко виявити традиційними методами.

Впровадження хмарних EDR-рішень, оскільки перехід до хмарних EDR-рішень дозволяє забезпечити гнучкість і масштабованість, необхідну для сучасних динамічних мереж. Хмарні EDR-рішення швидко розгортаються й оновлюються, що забезпечує постійний захист від нових загроз.

*Розширене виявлення та реагування на рівні мережі: к*рім захисту кінцевих пристроїв, сучасні EDR-системи можуть забезпечувати розширене виявлення та реагування на рівні мережі, що дозволяє виявляти та нейтралізувати загрози у всій мережі організації [32].

Отже, розширене виявлення та реагування (EDR) є потужною технологією, яка забезпечує глибокий аналіз активності на кінцевих пристроях і дозволяє виявляти та реагувати на складні загрози у реальному часі. EDR-системи забезпечують проактивний підхід до кібербезпеки, дозволяючи організаціям швидко реагувати на інциденти, мінімізувати збитки та забезпечувати високий рівень захисту від сучасних загроз. Впровадження EDR-систем є критичним кроком для організацій, які прагнуть підвищити свою мережеву безпеку й забезпечити надійний захист своїх інформаційних систем.

2.4 Системи управління інформацією та подіями безпеки (SIEM)

Системи управління інформацією та подіями безпеки (Security Information and Event Management. SIEM) є комплексними рішеннями, які забезпечують централізований моніторинг, виявлення та управління інцидентами безпеки у реальному часі. SIEM-системи об'єднують функції збору, аналізу та кореляції даних з різних джерел, що дозволяє організаціям ефективно виявляти та реагувати на загрози.

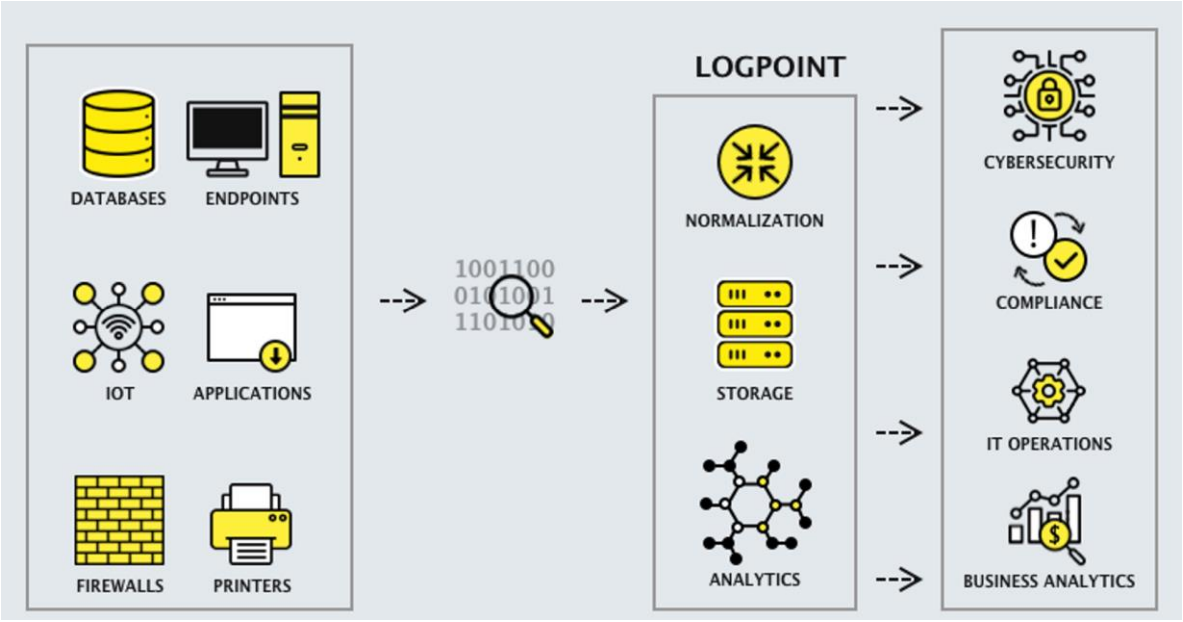

Рис. 2.8. Схема системи управління інформаціє та подіями безпеки

Основні компоненти SIEM-систем

Збір даних. SIEM-системи збирають дані з різних джерел, таких як журнали подій, мережеві пристрої, сервери, кінцеві точки, додатки та бази даних. Це можуть бути як структуровані, так і неструктуровані дані, що надають повну картину активності у мережі. Джерела даних включають фаєрволи, антивірусні програми, системи виявлення та запобігання вторгнень (IDS/IPS), системи керування доступом, VPN, проксі-сервери та інші засоби безпеки. Сучасні SIEM можуть також інтегруватися з хмарними сервісами та IoT-пристроями, збираючи дані з цих джерел для забезпечення всебічного моніторингу.

Нормалізація даних. Зібрані дані нормалізуються, тобто приводяться до єдиного формату, що полегшує їх подальший аналіз та кореляцію. Це необхідно для забезпечення узгодженості та порівнянності даних з різних джерел. Нормалізація дозволяє ефективніше аналізувати дані та знижує ризик помилок при обробці великої кількості різнорідних подій.

Аналіз і кореляція даних. SIEM-системи використовують різні методи аналізу даних, включаючи сигнатурний аналіз, евристичний аналіз та поведінковий аналіз. Кореляція подій дозволяє виявляти складні атаки, які можуть залишатися непоміченими при аналізі окремих подій. Методи машинного навчання можуть застосовуватись для вдосконалення аналізу та виявлення аномалій на основі поведінкових шаблонів. Наприклад, кореляція подій може включати аналіз одночасних спроб доступу до мережі з різних географічних місць, що може свідчити про компрометацію облікових даних.

Управління інцидентами. SIEM-системи надають інструменти для управління інцидентами безпеки, включаючи створення та відстеження інцидентів, призначення відповідальних осіб, документування заходів реагування та контроль за їх виконанням. Це дозволяє забезпечити ефективне управління інцидентами, від їх виявлення до завершення розслідування та усунення наслідків. Автоматизація управління інцидентами за допомогою SOAR (Security Orchestration, Automation, and Response) платформ дозволяє швидко реагувати на інциденти та мінімізувати їх вплив.

Звітування й забезпечення відповідності. SIEM-системи генерують детальні звіти про інциденти безпеки, що дозволяє організаціям оцінювати ефективність своїх заходів безпеки та відповідати вимогам нормативних актів та стандартів (наприклад, GDPR, PCI DSS, HIPAA). Звітування може включати інформацію про виявлені загрози, вжиті заходи та результати розслідувань. SIEM-системи також надають інструменти для аудиту, що дозволяє організаціям демонструвати відповідність вимогам регуляторів [33].

Функції SIEM, які мають на меті виявлення загроз, охоплюють:

Моніторинг у реальному часі. SIEM-системи забезпечують постійний моніторинг активності у мережі та на кінцевих пристроях у режимі реального часу. Це дозволяє швидко виявляти підозрілу активність та загрози. Моніторинг включає відстеження подій з різних джерел, таких як фаєрволи, IDS/IPS, антивіруси, сервери, додатки та бази даних. У випадку виявлення підозрілої активності SIEM-система автоматично генерує оповіщення й запускає процес реагування.

Кореляція подій. SIEM-системи використовують кореляцію подій для виявлення складних і багатоступеневих атак. Кореляція полягає у поєднанні окремих подій у єдиний контекст для виявлення загроз, які можуть бути непоміченими при окремому аналізі. Кореляція дозволяє виявляти аномалії та відхилення від нормальної поведінки, що може свідчити про атаку або порушення безпеки. Наприклад, кореляція може поєднувати дані про невдалі спроби входу до системи, незвичайні зміни у привілеях користувача та підозрілу мережеву активність для виявлення компрометації облікових даних.

Функція аналізу SIEM-систем забезпечує детальне вивчення й оцінку подій та інцидентів безпеки, зокрема аналіз журналів, відстеження активності користувачів та пристроїв, а також виявлення причин і наслідків інциденту. Інструменти аналізу включають пошук, фільтрацію, кореляцію подій, візуалізацію даних та створення звітів. Сучасні SIEM-системи можуть використовувати інтерактивні панелі для візуалізації даних та спрощення аналізу інцидентів.

Звітування та відповідність вимогам:

SIEM-системи генерують детальні звіти про інциденти безпеки, що дозволяє організаціям оцінювати ефективність своїх заходів безпеки та відповідати вимогам нормативних актів та стандартів. Звіти можуть включати інформацію про виявлені загрози, вжиті заходи, результати розслідувань, а також оцінку відповідності вимогам нормативних актів та стандартів. SIEM-системи також можуть генерувати спеціалізовані звіти для різних аудиторій, включаючи технічних фахівців, керівництво та регуляторів [34].

Завдяки використання систем SIEM організація отримає низку важливих переваг, зокрема:

*Здійснення централізованого моніторингу вс*іх подій безпеки в організації, що дозволяє отримати повну картину про стан безпеки та швидко реагувати на загрози. Централізований моніторинг дозволяє об'єднати дані з різних джерел та забезпечити їхній ефективний аналіз, а, отже, зменшити час реагування на інциденти та покращити координацію заходів безпеки.

Раннє виявлення загроз до того, як вони можуть завдати значної шкоди. Завдяки цьому організація забезпечує проактивний підхід до мережевої безпеки. Раннє виявлення загроз дозволяє мінімізувати ризики та запобігти інцидентам безпеки. Наприклад, виявлення підозрілої активності на ранній стадії може запобігти компрометації системи або крадіжці даних.

Комплексний аналіз і кореляція подій дозволяє виявляти складні та багатоступеневі атаки, які можуть бути непоміченими при окремому аналізі, отримати повну картину про інциденти безпеки та їхні причини, виявляти приховані загрози та забезпечувати ефективний захист.

SIEM-системи забезпечують організації *відповідність вимогам нормативних актів і стандартів*, що є критичним чинником для багатьох організацій, особливо у регульованих державою галузях. Наприклад, SIEM-системи можуть допомогти забезпечити відповідність вимогам законодавства щодо захисту персональних даних.

Водночас SIEM системам притаманні низка недоліків і труднощів, пов’язаних із їх впровадженням і забезпеченням належного функціонування.

Впровадження SIEM-систем може бути *складним завданням*, що вимагає значних ресурсів та високого рівня експертизи. Це може включати налаштування збору даних, нормалізації, кореляції подій і правил безпеки. Складність впровадження може бути перешкодою для малих і середніх організацій без достатньої кількості фахівців з безпеки. Впровадження SIEM-системи може вимагати тісної співпраці з усіма підрозділами організації для забезпечення збору необхідних даних.

SIEM-системи є досить *дороговартісними у впровадженні та супроводі*, особливо для великих організацій з великою кількістю джерел даних і високими вимогами до безпеки. Висока вартість може бути перешкодою для деяких організацій, особливо малого та середнього бізнесу. Окрім первинних витрат на впровадження, організації можуть стикатися з постійними витратами на обслуговування й оновлення SIEM-системи.

SIEM-системи можуть генерувати *велику кількість хибних спрацьовувань*, що вимагає додаткових зусиль для їхньої перевірки та фільтрації. Велика кількість фальшивих спрацьовувань може ускладнювати роботу фахівців з безпеки та знижувати ефективність реагування на справжні загрози. Налаштування правил кореляції та фільтрації може вимагати значних зусиль для зменшення кількості фальшивих спрацьовувань [35].

Виділяють такі тенденції розвитку сучасних систем SIEM:

Сучасні SIEM-системи часто інтегруються з іншими засобами кібербезпеки, такими як EDR, SOAR, та антивірусні програми, для забезпечення комплексного захисту. Інтеграція дозволяє отримувати більш повну картину про загрози, інциденти безпеки та швидше реагувати на загрози.

Використання технологій *штучного інтелекту та машинного навчання* дозволяє покращити точність виявлення загроз, автоматизувати рутинні завдання і знизити кількість хибних спрацювань. Машинне навчання допомагає створювати більш точні моделі поведінки та виявляти складні атаки, які важко

виявити традиційними методами. Використання AI/ML може значно підвищити ефективність SIEM-систем і зменшити навантаження на фахівців з безпеки.

Перехід до *хмарних SIEM-рішень* забезпечує гнучкість і масштабованість, необхідну для сучасних динамічних мереж. Хмарні SIEM-рішення можуть бути швидко розгорнуті та оновлені, що забезпечує постійний захист від нових загроз. Хмарні рішення можуть бути особливо корисними для організацій з розподіленими офісами та віддаленими працівниками.

Використання платформ *автоматизації та оркестрації* (SOAR, Security Orchestration, Automation, and Response) для автоматизації та оркестрації процесів мережевої безпеки дозволяє підвищити ефективність її управління. Автоматизація дозволяє швидко реагувати на загрози, мінімізувати час на виконання рутинних завдань і підвищити загальну ефективність заходів безпеки. SOAR платформи можуть автоматизувати процеси управління загрозами.

Отже, системи управління інформацією та подіями безпеки (SIEM) є критичним компонентом сучасної стратегії мережевої безпеки. Вони забезпечують централізований моніторинг, виявлення загроз та управління інцидентами безпеки у реальному часі. SIEM-системи об'єднують функції збору, аналізу та кореляції даних з різних джерел, що дозволяє організаціям ефективно виявляти та реагувати на загрози. Впровадження SIEM-систем є важливим кроком для організацій, які прагнуть підвищити свою мережеву безпеку й забезпечити надійний захист своїх інформаційних систем.

Висновки до розділу 2

Встановлено, що для ефективного забезпечення мережевої безпеки сучасні організації повинні впроваджувати проактивний підхід до захисту мережі, який спрямований на запобігання новим загрозам і кібервикликам. Ці завдання у комплексі виконують різні технології виявлення загроз мережевій безпеці, зокрема міжмережеві екрани, віртуальні приватні мережі, антивірусні програми, системи виявлення та запобігання вторгненням (IDS/IPS), захисту від витоку

даних (DLP), захисту веб-доступу й електронної пошти, засоби аналізу поведінки, аналізу мережевого трафіку (NTA), розширеного виявлення та реагування (EDR), системи управління інформацією та подіями безпеки (SIEM) тощо.

Проведений аналіз показав, що системи виявлення й запобігання вторгнень (IDS/IPS) є важливим компонентом забезпечення мережевої безпеки організації, оскільки вони надають можливість раннього виявлення загроз і моніторингу мережевого трафіку.

Ще одним критичним елементом забезпечення мережевої безпеки є технології розширеного виявлення та реагування (EDR), які забезпечують глибокий аналіз активності на кінцевих пристроях і дозволяють виявляти й реагувати на складні загрози у реальному часі. Впровадження хмарних EDR-рішень додає гнучкості та масштабованості, що є важливим для динамічних мереж. Крім того, сучасні EDR-системи забезпечують розширене виявлення та реагування на рівні мережі, що дозволяє забезпечити всебічний захист.

Системи управління інформацією та подіями безпеки (SIEM) відіграють важливу роль у забезпеченні комплексного моніторингу й управління мережевою безпекою. SIEM-системи дозволяють збирати, аналізувати й корелювати дані з різних джерел, що забезпечує централізований моніторинг і швидке виявлення загроз безпеці. Основними перевагами SIEM-систем є можливість раннього виявлення загроз, централізованого моніторингу, комплексного аналізу і кореляції подій, підтримка нормативної відповідності.

Дослідження технологій IDS/IPS, EDR та SIEM, які виконують завдання виявлення загроз мережевій безпеці, показало, що організаціям доцільно використовувати комбінований підхід до забезпечення мережевої безпеки відповідно до потреб і можливостей конкретної організації, інтегруючи різні технології виявлення загроз для забезпечення багаторівневого захисту мережі.

Розділ 3 ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТЕХНОЛОГІЙ ВИЯВЛЕННЯ ЗАГРОЗ МЕРЕЖЕВІЙ БЕЗПЕЦІ

3.1 Поняття й основні показники ефективості технологій виявлення загроз

Як відзначалося вище в роботі, технології виявлення загроз мережевій безпеці відіграють важливу роль у запобіганні потенційним деструктивним чинникам, які можуть негативно вплинути на стан захищеності мережевих ресурсів компанії. Водночас, основоположним принципом забезпечення інформаційної безпеки загалом і мережевої безпеки зокрема є економічна обґрунтованість, тобто, у випадку технологій виявлення загроз, витрати на придбання, встановлення, оновлення, забезпечення кваліфікованим персоналом, обслуговування тощо не повинні перевищувати можливі збитки внаслідок реалізації загроз.

У цьому контексті доцільно розглянути питання ефективності технологій виявлення загроз мережевій безпеці. Дослідження показало наявність різних підходів до розуміння сутності поняття «ефективність». Так, відповідно до стандарту ISO 9000:2015 Системи управління якістю – Основні положення та словник термінів *ефективність* – це співвідношення між досягненим результатом і використаними ресурсами [36]. Науковці переважно також поділяють це бачення. Тим не менше, деякі дослідники ефективності роблять акцент на здатності приносити ефект, результативність процесу, проекту тощо [37].

У даній роботі ефективність технологій виявлення загроз мережевій безпеці охоплюватиме сукупність таких основних показників (Рис. 3.1) [38]:

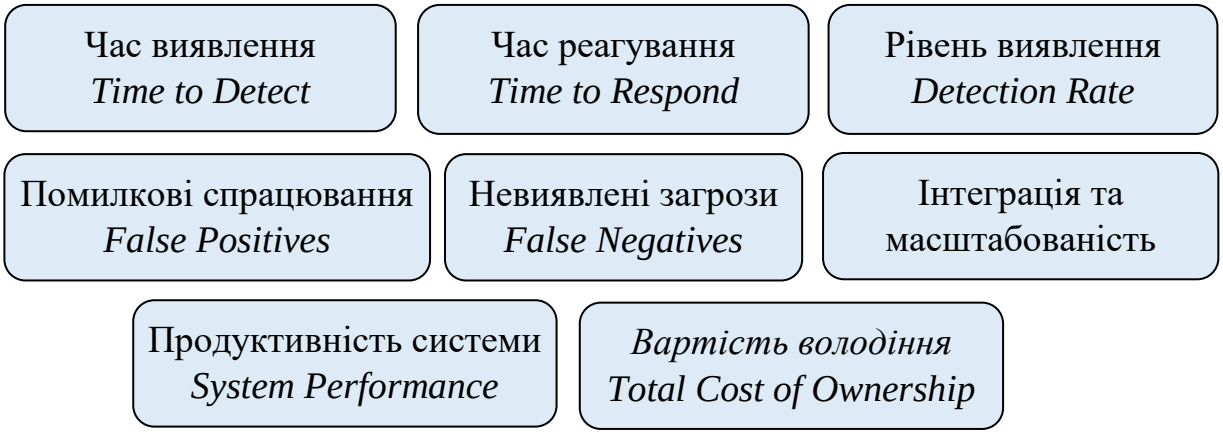

Рис. 3.1. Показники ефективності технологій виявлення загроз мережевій безпеці

Крім основних показників ефективність зазначених технологій можна оцінювати через можливості аналітики та звітності, інтерактивні дашборди (Interactive Dashboards), освіченість і кваліфікованість персоналу, використання штучного інтелекту (AI) та машинного навчання (ML).

Розглянемо сутність перелічених показників ефективності.

Час виявлення (Time to Detect, TTD)

Час виявлення (TTD) вимірює, скільки часу проходить від моменту, коли загроза з'являється в мережі, до моменту її виявлення системою безпеки. Чим менше часу потрібно на виявлення, тим менше шкоди може завдати загроза.

Для зменшення TTD використовують методи зменшення прогнозуючого аналізу й кореляції подій.

Прогнозна аналітика (Predictive Analytics) передбачає використання алгоритмів машинного навчання для аналізу історичних даних і виявлення патернів, які можуть свідчити про потенційні загрози, а також розробку моделей, що прогнозують появу загроз на основі аномалій в мережевому трафіку.

Метод кореляція подій (Event Correlation) охоплює збір та аналіз даних з різних джерел, таких як журнали подій, мережеві сенсори й системи моніторингу. Доцільним є використання систем SIEM (Security Information and Event Management), які можуть автоматично корелювати події та виявляти загрози на ранніх етапах.

Час реагування (Time to Respond, TTR)

Час реагування (TTR) вимірює, скільки часу потрібно команді безпеки, щоб відреагувати на виявлену загрозу. Чим швидше команда реагує, тим менше шкоди може завдати загроза.

Щоб зменшити TTR доцільно використовувати системи оркестрації та автоматизації безпеки (Security Orchestration and Automation, SOAR), які забезпечують автоматизацію процесів реагування на інциденти, включаючи збір даних, аналіз та виконання дій з нейтралізації загроз, а також автоматизацію рутинних завдань, що дозволяє зменшити навантаження на команду безпеки та скоротити час реагування.

Процедури реагування (Incident Response Playbooks) використовують для зменшення часу реагування, оскільки вони передбачають розробку детальних сценаріїв реагування на різні типи загроз з описом послідовності дій для швидкого й ефективного реагування, регулярне тестування й оновлення сценаріїв для врахування нових загроз та змін у мережевій інфраструктурі.

Рівень виявлення (Detection Rate)

Рівень виявлення показує, яку частку загроз система безпеки здатна виявити з загальної кількості спроб атак. Високий рівень виявлення свідчить про надійність системи.

Для підвищення рівня виявлення використовують системи розширеного виявлення та реагування (Extended Detection and Response, XDR), які здатні інтегрувати дані з різних джерел, включаючи кінцеві точки, мережу, хмарні сервіси та інші системи безпеки і таким чином покращити видимість загроз та підвищення точності виявлення.

Додатковими засобами підвищення показників виявлення є сигнатурний і поведінковий аналіз (Signature-Based and Behavioral Analysis). Сигнатурний аналіз базується на виявленні відомих сигнатур загроз, що дозволяє швидко ідентифікувати відомі атаки, а поведінковий аналіз відстежує аномалії в поведінці користувачів і систем, які можуть свідчити про нові або невідомі загрози.

Помилкові спрацювання (False Positives)

Помилкові спрацювання – це випадки, коли система помилково ідентифікує легітимну активність як загрозу. Велика кількість помилкових спрацювань може призвести до «втоми від попереджень» у команди безпеки, що знижує її ефективність.

Методами зменшення кількості помилкових спрацювань є контекстуалізація загроз і застосування адаптивних алгоритмів.

Контекстуалізація загроз (Threat Contextualization) передбачає використання додаткових даних для контекстуалізації загроз, що дозволяє точніше визначати, чи є активність загрозою, а також застосування технологій, що аналізують поведінку користувачів, історію взаємодії та інші чинники зниження кількості помилкових спрацювань.

З метою зменшення кількості помилкових спрацювань доцільним є використання адаптивних алгоритмів (Adaptive Algorithms), які навчаються на основі зворотного зв'язку від команди безпеки й автоматично коригують свої моделі, застосовують методи машинного навчання для постійного вдосконалення процесу виявлення загроз.

Помилкові пропуски загроз (False Negatives)

Помилкові пропуски загроз трапляються, коли система не виявляє реальну загрозу. Це є однією з найсерйозніших проблем, оскільки невиявлені загрози можуть завдати значної шкоди.

Для мінімізації випадків невиявлення загроз використовують поглиблений аналіз загроз (Deep Threat Analysis), який застосовує методи глибокого навчання для аналізу складних патернів загроз, які можуть бути пропущені традиційними методами, та інтегрують аналіз на різних рівнях системи безпеки для забезпечення багаторівневого виявлення загроз.

Багаторівневий захист (Multi-Layered Defense) завдяки використанню кількох рівнів захисту, включаючи мережеві фаєрволи, IDS/IPS, EDR та інші засоби, підвищує показник виявлення загроз. Застосування стратегії поглибленого (ешелованого) захисту (Defense-in-Depth), який охоплює різні

методи та засоби безпеки на різних рівнях мережі, також сприяє зниженню рівня помилкових пропусків мережевих загроз.

Продуктивність системи (System Performance)

Показник продуктивності системи безпеки показує, як впливають технології виявлення загроз на загальну продуктивність мережі. Надмірне навантаження може уповільнити роботу мережі та знизити її ефективність.

Методами покращення продуктивності системи є аналіз впливу й технології оптимізації.

Аналіз впливу (Impact Analysis) передбачає оцінку впливу системи виявлення загроз на продуктивність мережі та застосунків для виявлення потенційних вузьких місць, а також використання аналітичних інструментів для вимірювання продуктивності та ідентифікації ділянок, де можна оптимізувати систему.

Використання технологій оптимізації (Optimization Technologies), зокрема засобів кешування та розподіленої обробки даних і рішень для обробки даних на периферії (edge computing), сприяє зменшення навантаження на систему безпеки та підвищенню швидкості й ефективності аналізу загроз відповідно.

Інтеграція та масштабованість

Ефективні системи виявлення загроз безпеці мережі повинні легко інтегруватися з існуючою інфраструктурою та бути масштабованими відповідно до зростаючих потреб підприємства. Для покращення інтеграції та масштабованості використовують модульні архітектури (Modular Architectures), що дозволяють легко додавати або змінювати компоненти системи безпеки без значного впливу на роботу всієї системи і можуть бути інтегровані з іншими системами безпеки та мережевими інструментами. Використання хмарних рішень також забезпечують гнучку масштабованість та інтеграцію з іншими хмарними сервісами, дають змогу легко масштабувати ресурси відповідно до потреб безпеки підприємства.

Вартість володіння (Total Cost of Ownership, TCO)

Оцінка ТСО включає всі витрати на впровадження, експлуатацію та підтримку технологій виявлення загроз, зокрема витрати на обладнання, програмне забезпечення, навчання персоналу та підтримку.

Методи оцінки ТСО охоплюють планування витрат (Cost Planning) з детальним аналізом і плануванням витрат на впровадження, експлуатацію та підтримку системи безпеки, використанням фінансових моделей для оцінки витрат на кожному етапі життєвого циклу системи, а також аналіз повернення інвестицій від впровадження системи безпеки ROI (Return on Investment), який включає порівняння витрат на різні рішення для визначення найбільш економічно вигідного варіанту.

У таблиці 3.1 показано перелік основних показників ефективості безпеки й технологій, які сприяють їхньому покращенню.

Таблиця 3.1.

Основні показники ефективості безпеки й технології їх покращення

Показник	Засоби покращення
Час виявлення (Time to Detect, TTD)	Прогнозна аналітика (Predictive Analytics) Метод кореляція подій (Event Correlation)
Час реагування (Time to Respond, TTR)	Системи оркестрації та автоматизації безпеки (Security Orchestration and Automation, SOAR) Процедури реагування (Incident Response Playbooks)
Рівень виявлення (Detection Rate)	Системи розширеного виявлення та реагування (Extended Detection and Response, XDR) Сигнатурний і поведінковий аналіз (Signature-Based and Behavioral Analysis)
Помилкові спрацювання (False Positives)	Контекстуалізація загроз (Threat Contextualization) Адаптивні алгоритми (Adaptive Algorithms)
Помилкові пропуски загроз (False Negatives)	Поглиблений аналіз загроз (Deep Threat Analysis) Багаторівневий захист (Multi-Layered Defense)

Продовження табл. 3.1.

Продуктивність системи (System Performance)	Аналіз впливу (Impact Analysis) Технології оптимізації (Optimization Technologies)
Інтеграція та масштабованість	Модульні архітектури (Modular Architectures) Хмарні технології (Cloud Technology)
Вартість володіння (Total Cost of Ownership, TCO)	Планування витрат (Cost Planning) Аналіз повернення інвестицій (Return on Investment, ROI)

Додатковими показниками оцінювання ефективності систем виявлення загроз мережевій безпеці є:

- Наявність розширених можливостей *аналітики та звітності*, що дозволяє підприємствам детально аналізувати загрози й ефективність реагування;
- Використання *інтерактивних інформаційних панелей (Interactive Dashboards)* для моніторингу стану безпеки в реальному часі та швидкого доступу до критичної інформації;
- Постійне *навчання та підвищення кваліфікації команди безпеки*, що є важливим аспектом ефективного використання технологій виявлення загроз;
- Використання *штучного інтелекту (AI) та машинного навчання (ML),* інтеграція яких дозволяє вдосконалювати алгоритми виявлення загроз, а отже, підвищити точність і зменшити кількість помилкових спрацювань.

3.2 Ефективність систем виявлення та запобігання вторгненням (IDS/IPS)

Ефективність систем виявлення та запобігання вторгненням (IDS/IPS) є критичним аспектом для забезпечення інформаційної безпеки в корпоративних мережах. Проаналізуємо ключові показники ефективності IDS/IPS, включаючи точність виявлення загроз, рівень хибних спрацювань, пропущених загроз і швидкість реакції на інциденти.

Точність виявлення загроз

Точність виявлення загроз (Detection Accuracy) є одним з головних показників ефективності IDS/IPS. За даними досліджень, сучасні IDS/IPS системи забезпечують точність виявлення в межах 85% до 95% для відомих загроз. Це означає, що система правильно ідентифікує від 85% до 95% реальних загроз, що надходять до мережі.

Хибні спрацювання

Хибні спрацювання (False Positives) охоплюють випадки, коли система ідентифікує безпечний трафік як потенційну загрозу. Для сучасних IDS/IPS систем цей показник варіюється в межах 5% до 15%. Високий рівень хибних спрацювань може призводити до перевантаження адміністраторів безпеки та втрати ресурсів на аналіз хибних сповіщень безпеки.

Пропущені загрози

Пропущені загрози (False Negatives) – це випадки, коли система не виявляє реальну загрозу. Рівень пропущених загроз зазвичай становить менше 10%, але може змінюватися залежно від якості сигнатур і методів поведінкового аналізу. Високий рівень пропущених загроз може мати серйозні наслідки для безпеки організації.

Швидкість реагування на загрози

Швидкість реакції на загрози (Response Time) є важливим фактором для ефективності IPS систем. Сучасні системи забезпечують відповідь у реальному часі, дозволяючи миттєво блокувати шкідливий трафік. Залежно від конкретної системи, час реакції може варіюватися від кількох секунд до кількох хвилин.

Найвищі показники ефективності показують антивірусні компоненти й засоби поведінкової аналітики в IDS/IPS. Так, антивірусні модулі, інтегровані в IDS/IPS, показують ефективність виявлення від 90% до 95% для відомих загроз за даними незалежних тестувань. Засоби, що використовують поведінковий аналіз і машинне навчання, можуть досягати ефективності до 98% у виявленні аномалій і нових загроз.

Згідно з тестами NSS Labs, різні IDS/IPS системи показують ефективність в межах 85-95% у виявленні відомих загроз. У реальних умовах підприємства при правильному налаштуванні й регулярному оновленні ефективність може досягати і перевищувати 90% [39].

Отже, як свідчить аналіз, ефективність систем IDS/IPS є високою, проте вона залежить від багатьох факторів, включаючи правильну конфігурацію, регулярне оновлення й інтеграцію з іншими системами безпеки. Для досягнення максимальної ефективності у виявленні та запобіганні загрозам, важливо проводити регулярне тестування та налаштування системи.

3.3 Ефективність технологій розширеного виявлення та реагування (EDR)

Технології розширеного виявлення та реагування (Endpoint Detection and Response, EDR) стають все більш важливими для сучасних організацій завдяки їх здатності швидко та ефективно виявляти й реагувати на загрози. Ефективність EDR-систем залежить від таких ключових факторів, як точність виявлення, швидкість реагування, здатність до автоматизації та інтеграції з іншими системами безпеки.

Точність виявлення загроз

EDR-системи відомі своєю високою точністю виявлення загроз. Сучасні EDR-рішення використовують передові методи аналізу, включаючи машинне навчання та поведінковий аналіз, що дозволяє досягати точності виявлення до 99% для відомих і нових загроз. Це означає, що система правильно ідентифікує більшість реальних загроз, які можуть виникнути на кінцевих точках.

Швидкість реагування

Швидкість реагування є критичним показником ефективності EDR. Більшість сучасних EDR-систем забезпечують реагування в реальному часі, що дозволяє миттєво вжити заходів для нейтралізації загроз. Автоматизація

процесів реагування дозволяє значно скоротити час від виявлення до усунення загрози, зменшуючи потенційні збитки.

Хибні спрацювання

EDR-системи мають низький рівень хибних спрацювань (False Positives) завдяки використанню комбінованого підходу до виявлення загроз. Цей показник зазвичай становить менше 5%, що дозволяє уникнути перевантаження адміністраторів безпеки та зосередитися на реальних загрозах.

Автоматизація

Один з основних факторів ефективності EDR – це здатність до автоматизації процесів виявлення та реагування на загрози. EDR-системи можуть автоматично застосовувати політики безпеки, ізолювати підозрілі файли, блокувати шкідливі процеси й інформувати адміністраторів про інциденти. Це дозволяє значно підвищити швидкість та ефективність реагування на загрози.

Інтеграція з іншими системами безпеки

EDR-системи часто інтегруються з іншими інструментами кібербезпеки, такими як SIEM, антивірусні програми, фаєрволи та системи управління вразливостями. Це дозволяє створити комплексну систему захисту, яка забезпечує глибоке бачення та контроль над безпекою мережі.

Згідно з дослідженнями, EDR-системи можуть виявляти до 97% загроз, які інші засоби захисту зазвичай пропускають. У тестах, проведених незалежними лабораторіями, такими як AV-TEST [40] і MITRE, сучасні EDR-рішення показують високу ефективність у виявленні складних загроз, включаючи атаки нульового дня (zero-day attacks).

Таким чином, EDR-системи забезпечують високу ефективність у виявленні та реагуванні на загрози завдяки точності виявлення, швидкості реагування, низькому рівню хибних спрацювань, автоматизації процесів та інтеграції з іншими системами безпеки. Використання EDR дозволяє організаціям значно підвищити рівень захисту кінцевих точок і зменшити ризики, пов'язані з кіберзагрозами.

3.4 Ефективність систем управління інформацією та подіями безпеки (SIEM)

Система управління інформацією та подіями безпеки (Security Information and Event Management, SIEM) є важливим інструментом для моніторингу, аналізу та реагування на інциденти безпеки в реальному часі. Ефективність SIEM систем вимірюється за кількома ключовими показниками, зокрема точність виявлення загроз, хибні спрацювання, швидкість реагування і загальна інтеграція з іншими системами безпеки. Розглянемо середні показники ефективності SIEM систем [41].

Точність виявлення загроз

Точність виявлення загроз є критичним показником ефективності SIEM. Сучасні SIEM системи зазвичай досягають точності виявлення загроз на рівні 85-95%. Це означає, що система може правильно ідентифікувати більшість реальних загроз, які надходять до мережі, зокрема через використання передових методів аналізу та кореляції даних з різних джерел.

Хибні спрацювання

Показник хибних спрацювань (False Positives) є важливим для адміністраторів безпеки, оскільки висока кількість хибних тривог може призвести до перевантаження і втрати ресурсів. Сучасні SIEM системи здатні знижувати рівень хибних спрацювань до 5-15% завдяки складним правилам кореляції та поведінковому аналізу. Це дозволяє зменшити кількість помилкових сповіщень безпеки і зосередитися на реальних загрозах.

Пропущені загрози

Пропущені загрози (False Negatives) – це випадки, коли система не виявляє реальну загрозу. Середній показник пропущених загроз для SIEM систем зазвичай становить менше 10%, що вказує на високу ефективність у виявленні широкого спектру загроз, включаючи нові та складні атаки.

Швидкість реагування

Швидкість реагування на загрози є критично важливим показником ефективності SIEM. Завдяки автоматизації процесів реагування, таких як блокування підозрілих IP-адрес чи ізоляція заражених кінцевих точок, сучасні SIEM системи можуть значно скоротити час від виявлення до усунення загрози. Більшість систем SIEM забезпечують швидкість реагування в реальному часі або протягом кількох хвилин.

Інтеграція з іншими системами безпеки

Однією з основних переваг SIEM систем є їх здатність інтегруватися з іншими інструментами кібербезпеки, такими як IDS/IPS, EDR, антивірусні програми, фаєрволи та системи управління вразливостями. Це дозволяє створити комплексну систему захисту, що значно підвищує ефективність моніторингу й реагування на загрози.

Згідно з дослідженнями, проведеними аналітичними компаніями, такими як Gartner та Forrester [42], ефективність SIEM систем в реальних умовах демонструє такі показники:

- Точність виявлення загроз: 85-95%
- Зниження хибних спрацювань: до 10%
- Швидкість реагування: в реальному часі або протягом кількох хвилин
- Зниження часу на розслідування інцидентів: до 70%

Отже, SIEM системи є потужним інструментом для забезпечення мережевої безпеки завдяки їх здатності збирати, корелювати й аналізувати дані з різних джерел. Вони забезпечують високу ефективність у виявленні загроз, зниженні хибних спрацювань, швидкості реагування та інтеграції з іншими системами безпеки. Використання SIEM дозволяє організаціям підвищити рівень захисту від кіберзагроз і забезпечити оперативне реагування на інциденти.

Підсумки та порівняння ефективності IDS/IPS, EDR та SIEM

Аналіз ефективності систем IDS/IPS, EDR та SIEM демонструє, що кожна з них має свої унікальні переваги та недоліки. У таблиці 3.2 наведено порівняння ключових показників ефективності цих систем [44].

Таблиця 3.2.

Порівняння показників ефективності технологій виявлення загроз мережевій безпеці

Показник	**IDS/IPS**	**EDR**	**SIEM**
Точність виявлення	85-95%	До 99%	85-95%
Хибні спрацювання	5-15%	Менше 5%	5-15%
Пропущені загрози	Менше 10%	Менше 3%	Менше 10%
Швидкість реагування	В реальному часі або кілька хвилин	В реальному часі	В реальному часі або кілька хвилин
Автоматизація	Обмежена	Висока	Висока
Інтеграція з іншими системами	Висока	Висока	Висока

Рекомендації щодо використання технологій виявлення загроз мережевій безпеці

Для досягнення максимальної ефективності у забезпеченні інформаційної безпеки рекомендується використовувати IDS/IPS, EDR та SIEM системи разом. Ось кілька стратегій для їх оптимального використання:

Комплексний захист: IDS/IPS можуть забезпечувати глибокий моніторинг мережевого трафіку та виявлення загроз на периметрі мережі, тоді як EDR системи забезпечують захист кінцевих точок і реагування на загрози в реальному часі. SIEM системи інтегрують дані з IDS/IPS та EDR для комплексного аналізу та кореляції подій.

Зниження кількості хибних спрацювань: Використання систем IDS/IPS та EDR разом дозволяє знизити число хибних спрацювань і пропущених загроз завдяки комбінованому підходу до виявлення загроз.

Автоматизація реагування: Високий рівень автоматизації систем EDR та SIEM у поєднанні з можливостями IDS/IPS забезпечує швидке й ефективне реагування на загрози.

Інтеграція з іншими системами безпеки: Інтеграція IDS/IPS, EDR та SIEM з іншими системами кібербезпеки створює комплексну систему захисту, що підвищує загальну ефективність мережевої безпеки організації.

Висновки до розділу 3

У сучасному світі кіберзагроз забезпечення ефективного захисту мережевої інфраструктури є критичним для безпеки організацій. Технології виявлення загроз, такі як системи виявлення та запобігання вторгненням (IDS/IPS), розширеного виявлення та реагування (EDR), управління інформацією та подіями безпеки (SIEM), є ключовими елементами забезпечення високого рівня мережевої безпеки.

Ефективність цих систем оцінюється за різними показниками, такими як час виявлення (TTD), час реагування (TTR), рівень виявлення, кількість помилкових спрацювань і пропущених загроз, продуктивність системи, інтеграція та масштабованість, а також вартість володіння (TCO). Використання сучасних технологій, таких як прогнозуючий аналіз, машинне навчання, штучний інтелект і методи обробки великих даних, дозволяє значно підвищити точність і швидкість виявлення загроз, зменшити кількість помилкових спрацювань і оптимізувати витрати на експлуатацію систем.

Додаткові аспекти, такі як розширені можливості аналітики та звітності, інтерактивні інформаційні панелі для моніторингу стану безпеки в реальному часі, постійне навчання та розвиток персоналу, а також використання AI та ML для вдосконалення алгоритмів виявлення загроз, є невід'ємною частиною забезпечення високої ефективності систем безпеки мережі.

Для досягнення максимальної ефективності у забезпеченні інформаційної безпеки рекомендується використовувати технології IDS/IPS, EDR та SIEM разом. Інтеграція цих систем дозволяє створити багаторівневий підхід до захисту, де кожен рівень доповнює інші, забезпечуючи більш повну і точну картину стану безпеки мережі. SIEM системи збирають та аналізують дані з

IDS/IPS і EDR, надаючи централізовану видимість і кореляцію подій для швидкого виявлення складних загроз. Це дозволяє оперативно реагувати на інциденти і приймати обґрунтовані рішення щодо нейтралізації загроз.

Загалом, інтеграція різних систем безпеки, їх постійне вдосконалення та адаптація до нових загроз дозволяють підприємствам забезпечувати надійний захист своїх мережевих ресурсів та інформаційних систем, знижуючи ризики та збитки від потенційних кібератак. Використання комплексного підходу до кібербезпеки, який включає в себе інтеграцію IDS/IPS, EDR та SIEM, є найбільш ефективним способом забезпечення всебічного захисту мережі та інформаційних активів підприємства.

ВИСНОВКИ

Дослідження показало, що мережева безпека є комплексом заходів, що забезпечують захист інформації та ресурсів мережі від різноманітних загроз на фізичному, адміністративному й технічному рівнях. Основними видами загроз мережевій безпеці є фізичні, логічні, загрози соціальної інженерії, цільові атаки (APT), внутрішні загрози. Методи атак на мережеву безпеку охоплюють шкідливе ПЗ, фішинг, ботнети, DoS /DDoS-атаки, атака типу «Man-in-the-Middle», аналіз пакетів, підміна DNS і IP-адреси тощо.

Встановлено, що методи й технології запобігання і протидії мережевим загрозам поділяють на заходи мережевої безпеки на пристроях користувачів і серверах. Основними заходами мережевої безпеки на пристроях користувачів є контроль доступу до мережі (NAC), віртуальні приватні мережі (VPN), захист від шкідливих програм, багатофакторна автентифікація. Заходи мережевої безпеки на серверах охоплюють використання міжмережевих екранів, систем виявлення вторгнень (IDS), засобів запобігання втраті даних (DLP), захищених вебшлюзів.

З’ясовано, що для ефективного забезпечення мережевої безпеки сучасні організації повинні впроваджувати проактивний підхід до захисту мережевих активів, який спрямований на запобігання новим загрозам і кібервикликам. Ці завдання у комплексі виконують різні технології виявлення загроз мережевій безпеці, зокрема міжмережеві екрани, віртуальні приватні мережі, антивірусні програми, системи виявлення та запобігання вторгненням (IDS/IPS), захисту від витоку даних (DLP), захисту веб-доступу й електронної пошти, засоби аналізу поведінки й мережевого трафіку (NTA), розширеного виявлення та реагування (EDR), системи управління інформацією та подіями безпеки (SIEM) тощо.

Проведений аналіз показав, що системи виявлення й запобігання вторгнень (IDS/IPS) є важливим компонентом забезпечення мережевої безпеки організації, оскільки вони надають можливість раннього виявлення загроз і моніторингу мережевого трафіку. Технології розширеного виявлення та реагування (EDR) забезпечують глибокий аналіз активності на кінцевих пристроях і дозволяють

виявляти й реагувати на складні загрози у реальному часі. Системи управління інформацією та подіями безпеки (SIEM) забезпечують можливість раннього виявлення загроз, централізованого моніторингу, комплексного аналізу і кореляції подій, підтримку нормативної відповідності.

За підсумками дослідження зроблено висновок, що організаціям доцільно використовувати комбінований підхід до забезпечення мережевої безпеки відповідно до потреб і можливостей конкретної організації, інтегруючи різні технології виявлення загроз для забезпечення багаторівневого захисту мережі.

Встановлено, що аналіз ефективності систем виявлення мережих загроз здійснюється за такими показниками як час виявлення (TTD), час реагування (TTR), рівень виявлення, кількість помилкових спрацювань і пропущених загроз, продуктивність системи, інтеграція і масштабованість, вартість володіння (TCO). Використання сучасних технологій, таких як прогнозуючий аналіз, машинне навчання, штучний інтелект і методи обробки великих даних, дозволяє значно підвищити точність і швидкість виявлення загроз, зменшити кількість помилкових спрацювань і оптимізувати витрати на експлуатацію систем.

Додаткові аспекти, такі як розширені можливості аналітики та звітності, інтерактивні інформаційні панелі для моніторингу стану безпеки в реальному часі, постійне навчання та розвиток персоналу, а також використання AI та ML для вдосконалення алгоритмів виявлення загроз, є невід'ємною частиною забезпечення високої ефективності систем безпеки мережі.

Для досягнення максимальної ефективності у забезпеченні інформаційної безпеки рекомендується використовувати технології IDS/IPS, EDR та SIEM разом. Інтеграція цих систем дозволяє створити багаторівневий підхід до мережевої безпеки, де кожен рівень доповнює інші, забезпечуючи більш повну і точну картину стану безпеки мережі, знижуючи ризики та збитки від потенційних кібератак, гарантуючи всебічний захист мережі та інформаційних активів підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. The Role of Physical Security. *EC-Council*. URL: https://www.eccouncil.org/ cybersecurity-exchange/network-security/role-of-physical-security-in-network-security/

2. Administrative Security. *Firewall Times.* URL: https://firewalltimes.com/ administrative-security-controls/

3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Preview. URL: https://www.iso.org/standard/82875.html

4. Реагування на інциденти URL: https://www.crowdstrike.com/ cybersecurity-101/incident-response/incident-response-steps/

5. What is a firewall? *CloudFlare.* URL: https://www.cloudflare.com/ learning/security/what-is-a-firewall/

6. ЩО таке IDS і IPS? *Juniper*. URL: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

7. VPN security. *CloudFlare.* URL: https://www.cloudflare.com/ learning/access-management/vpn-security/

8. Network security threats and vulnerabilities. NordLayer. URL: https://nordlayer.com/learn/network-security/threats/

9. What Are the Types of Physical Security? URL: https://www.bbrss.com/resources/news-blog/blogs/common-physical-security-threats

10. Social EngineeringWho, What, When and How? *University of Oxford.* URL: https://www.infosec.ox.ac.uk/article/social-engineering

11. What are insider threats. *IBM*. URL: https://www.ibm.com/topics/insider-threats

12. 17 Types of Cyber Attacks Commonly Used by Hackers. URL: https://www.aura.com/learn/types-of-cyber-attacks

13. What Is a Botnet? *Microsoft*. URL: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-a-botnet

14. What Is A Man-In-The-Middle (MitM)? *SentinelOne*. URL: https://www.sentinelone.com/cybersecurity-101/what-is-a-man-in-the-middle-mitm-attack-2/

15. What is IP spoofing? *CloudFlare*. URL: https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

16. Network Security. *CompTIA*. URL: https://www.comptia.org/content/guides/network-security-basics-definition-threats-and-solutions

17. Mccarty B. What are the Benefits of Using VPN Encryption? *Linford & Company LLP*. URL: https://linfordco.com/blog/vpn-encryption/

18. Multi-Factor Authentication (MFA). *CrowdStrike*. URL: https://www.crowdstrike.com/cybersecurity-101/multifactor-authentication-mfa/

19. What Is Data Loss Prevention? *IBM*. URL: https://www.paloaltonetworks.com/cyberpedia/data-loss-prevention

20. What is an Intrusion Detection System (IDS)? *IBM*. URL: https://www.ibm.com/topics/intrusion-detection-system

21. What is an Intrusion Prevention System (IPS)? In-Depth Guide. *SoftwareLab*. URL: https://softwarelab.org/blog/what-is-ips/

22. Behavioral Systems Analysis. URL: https://www.behavior.org/resources/395.pdf

23. What is Endpoint Detection and Response (EDR)? *Microsoft*. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response

24. What is Network Traffic Analysis? URL: https://blog.octobits.io/digital-transformation/what-is-network-traffic-analysis/

25. What Is a Honeypot? *CrowdStrike*. URL: https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/

26. What is security information and event management (SIEM)? *IBM*. URL: https://www.ibm.com/topics/siem

27. What is AI-Powered Behavioral Analysis. *CrowdStrike*. URL: https://www.crowdstrike.com/cybersecurity-101/secops/ai-powered-behavioral-analysis/

28. CS406: Information Security. URL: https://learn.saylor.org/mod/book/view.php?id=29820

29. IBM - What Are Advanced Persistent Threats? *CrowdStrike*. URL: https://www.ibm.com/topics/advanced-persistent-threats

30. Difference Between Firewall and IDS, IPS. *NextDoorSec*. URL: https://nextdoorsec.com/difference-between-firewall-and-ids/

31. What Is Endpoint Detection and Response. *Trellix*. URL: https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-detection-and-response/

32. What is endpoint detection and response (EDR). *IBM*. URL: https://www.ibm.com/topics/edr

33. Compliance with IBM Security QRadar SIEM. *IBM*. URL: https://www.ibm.com/products/qradar-siem/compliance

34. Benefits of Security Information and Event Management (SIEM). *Pendello*. URL: https://www.pendello.com/blog/benefits-of-security-information-and-event-management-siem-in-cybersecurity

35. Sheldon M. Villanueva Pros and Cons of Implementing SIEM. URL: https://www.itsasap.com/blog/pros-cons-siem

36. ДСТУ ISO 9000:2015 Системи управління якістю. Основні положення та словник термінів (ISO 9000:2015, IDT). URL: https://m.tntu.edu.ua/storage/pages/00000651/dstu9000-2015_osnovni_pol.slovnyk.pdf

37. Демченко А. О, Момот О. І. Про сутність понять "ефективність" та "результативність" в економіці. Економічний вісник Донбасу. 2013. № 3. С. 207-210. URL: http://nbuv.gov.ua/UJRN/ecvd_2013_3_29

38. Вимірювання ефективності контролю системи управління інформаційною безпекою на основі стандарту SNI ISO/IEC 27004: 2013. URL: https://iopscience.iop.org/article/10.1088/1757-899X/550/1/012020/meta

39. 2018 NSS Labs Next Generation Intrusion Prevention (NGIPS) Report. *Palo Alto*. URL: https://www.paloaltonetworks.com/resources/research/nss-labs-2018-ngips-test-report

40. Advanced EDR Test 2023: Bitdefender's Endpoint Security Tools. *AV-TEST*. *URL:* https://www.av-test.org/en/news/advanced-edr-test-2023-bitdefenders-endpoint-security-tools/

41. 2023 Report on State of SIEM Detection Risk. *CardinalOps*. URL: https://cardinalops.com/whitepapers/2023-report-on-state-of-siem-detection-risk/?#gf_20

42. How SIEM, EDR, and NDR complement each other. *Progress Flowmon*. URL: https://www.flowmon.com/en/blog/4-reasons-why-your-business-needs-network-detection-and-response-solutions

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)