Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

ННЦЗФН

Кафедра *інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти *другий (магістерський)*

Аналіз систем виявлення та запобігання вторгнень для захисту інформаційних мереж

(тема)

Виконала:
студентка *2* курсу, групи *ІМІзм-22-2*
Михайлова А.С.
(прізвище, ініціали)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-наукова*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)

Керівник *доц. к.т.н. Чеботарьова Д.В.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2024 р.

Не містить відомостей, заборонених до відкритого публікування

Студентка _____ *Михайлова А.С.*
(підпис) (прізвище та ініціали)

Керівник _____ *Чеботарьова Д.В.*
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки

ННЦЗФН

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)

Тип програми *Освітньо-наукова*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри ІМІ_____
(підпис)

"*20*" *червня* 2024р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці *Михайловій Анні Сергіївні*
(прізвище, ім'я, по батькові)

1. Тема роботи *Аналіз систем виявлення та запобігання вторгнень для захисту інформаційних мереж*

затверджені наказом по університету від "*27*" *березня* 2024 р. № *38 Стз*

2. Термін подання студентом роботи до екзаменаційної комісії *20 червня 2024 р.*

3. Вихідні дані до роботи *дослідити проблеми безпеки в інформаційних мережах, інструменти мережної безпеки, сучасні рішення IDS/IPS: Check Point Quantum, Cisco NGIPS, Hillstone Networks, OSSEC, Palo Alto Networks, Snort, Trellix (McAfee + FireEye), Trend Micro, Zeek (Bro) та ZScalar Cloud IPS; провести порівняльний аналіз цих рішень IDS/IPS.*

4. Перелік питань, що потрібно опрацювати в роботі

1. Засоби безпеки в інформаційних мережах.

2. Системи виявлення та запобігання вторгненням.

3. Огляд сучасних рішень IDS/IPS.

4. Порівняльний аналіз сучасних систем IDS/IPS.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____
Слайди у форматі Power Point (назва, мета та задачі роботи, основні результати роботи, висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*27.03.24*	*Виконано*
2	*Підбір літератури за темою роботи.*	*28.03 - 15.04.24*	*Виконано*
3	*Виконання розділу 1*	*16.04 - 30.04.24*	*Виконано*
4	*Виконання розділу 2*	*01.05 – 15.05.24*	*Виконано*
5	*Виконання розділу 3*	*16.05 – 31.05.24*	*Виконано*
6	*Виконання розділу 4*	*01.01 - 15.06.24*	*Виконано*
7	*Оформлення пояснювальної записки,*		
	презентаційного матеріалу та підготовка		
	до захисту у ЕК	*16.06 - 20.06.24*	*Виконано*

Дата видачі завдання *27 березня 2024 р.*

Студентка _____ *Михайлова А.С.*
(підпис) (прізвище, ініціали)

Керівник роботи _____ *доц. Чеботарьова Д.В.*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 85 с., 22 рис., 6 табл., 29 джерел, 2 додатки

Об'єкт дослідження – системи виявлення та запобігання вторгнень.

Мета роботи – дослідження та порівняння систем виявлення та запобігання вторгнень для захисту інформаційних мереж.

Результати – в роботі проаналізовано проблеми безпеки в інформаційних мережах, розглянуто інструменти мережної безпеки, засоби виявлення та усунення вразливостей, засоби виявлення та запобігання вторгнень. Досліджено класифікацію систем IDS/IPS, функціонал, архітектуру, принцип роботи, переваги та недоліки IDS/IPS. Виконано огляд та порівняльний аналіз найбільш популярних сучасних рішень IDS/IPS: Check Point Quantum, Cisco NGIPS, Hillstone Networks, OSSEC, Palo Alto Networks, Snort, Trellix (McAfee + FireEye), Trend Micro, Zeek (Bro) та ZScalar Cloud IPS. Проведено порівняння рішень IDS/IPS за основними характеристиками та виконано вибір кращих ріщень для різних ситуацій.

IDS, IPS, ІНФОРМАЦІЙНА МЕРЕЖА, БЕЗПЕКА, ВИЯВЛЕННЯ, ВТОРГНЕННЯ, ЗАПОБІГАННЯ, ЗАХИСТ, АТАКА, ЗАГРОЗА, АНОМАЛІЯ, СИГНАТУРА.

THE ABSTRACT

Explanatory note: 85 p., 22 fig., 6 tabl., 29 sources, 2 app.

Object of research - systems of detection and prevention of intrusions.

The purpose of the work is to research and comparison of intrusion detection and prevention systems for the protection of information networks.

Results - the work examines security problems in information networks were analyzed, network security tools, means of detecting and eliminating vulnerabilities, means of detecting and preventing intrusions were considered. The classification of IDS/IPS systems, functionality, architecture, principle of operation, advantages and disadvantages of IDS/IPS are studied. A review and comparative analysis of the most popular modern IDS/IPS solutions was performed: Check Point Quantum, Cisco NGIPS, Hillstone Networks, OSSEC, Palo Alto Networks, Snort, Trellix (McAfee + FireEye), Trend Micro, Zeek (Bro) and ZScalar Cloud IPS. A comparison of IDS/IPS solutions was carried out according to the main characteristics and the selection of the best solutions for different situations was carried out.

IDS, IPS, INFORMATION NETWORK, SECURITY, DETECTION, INTRUSION, PREVENTION, PROTECTION, ATTACK, THREAT, ANOMALY, SIGNATURE.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

ІМ – інформаційна мережа;

МН – машинне навчання;

ОС – операційна система;

ПЗ – програмне забезпечення;

ШІ – штучний інтелект;

C2 (Command and Control, C&C) – інфраструктура управління і контролю;

CASB (Cloud Access Security Broker) – брокер безпеки доступу до хмари;

CVE (Common Vulnerabilities and Exposures) – база даних загальновідомих вразливостей інформаційної безпеки;

DDoS (Distributed Denial-of-Service Attack) – розподілена атака на відмову в обслуговуванні;

DLP (Data Leak Prevention) – технологія запобігання витоку даних;

DNS (Domain Name System) – система доменних імен;

FTP (File Transfer Protocol) – протокол передачі файлів;

HIDS (Host-based Intrusion Detection System) – система виявлення вторгнень на хост;

HIPS (Host-based Intrusion Prevention System) – система запобігання вторгненням на основі хоста;

HTTP (Hyper Text Transfer Protocol) – протокол передачі гіпертексту;

IDS (Intrusion Detection System) – система виявлення вторгнень;

IMAP (Internet Message Access Protocol) – протокол доступу до інтернет-повідомлень;

IP (Internet Protocol) – інтернет протокол;

IPS (Intrusion Prevention System) – система запобігання вторгненням;

NBA (Network Behavior Analysis System) – система аналізу поведінки мережі;

NGFW (Next Generation Firewall) – брандмауер наступного покоління;

NGIPS (Next Generation IPS) – система запобігання вторгненням наступного покоління;

NIDS (Network-based Intrusion Detection System) – мережна система виявлення вторгнень;

NIPS (Network-based intrusion Prevention System) – мережна система запобігання вторгненням;

PCI DSS (Payment Card Industry Data Security Standard) – стандарт безпеки даних в індустрії платіжних карток;

POP (Post Office Protocol) – поштовий офісний протокол;

SAST (Static Application Security Testing) - статичне тестування безпеки програми;

SIEM (Security Information and Event Management) – інформація про безпеку та управління подіями;

SMTP (Simple Mail Transfer Protocol) простий протокол пересилання пошти;

SNMP (Simple Network Management Protocol) – простий протокол керування мережею;

SSL (Secure Socket Layer) – криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером;

TCP (Transmission Control Protocol) – протокол управління передачею;

TLS (Transport Layer Security) – захист на транспортному рівні;

URL (Uniform Resource Locator) – уніфікований локатор ресурсу;

VPN (Virtual Private Network) – віртуальна приватна мережа;

WIPS (Wireless Intrusion Prevention System) – система запобігання безпроводовому вторгненню.

ВСТУП

В наш час інформаційні мережі (ІМ) стрімко розвиваються, з кожним днем вони стають все більшими та складнішими. В інформаційних мережах з'являються нові послуги, а інноваційні інструменти зв'язку спрощують віддалену роботу. Змінюються методи зберігання даних, і тому з'являються нові активи для захисту. Через цей розвиток також постійно модернізуються, ускладнюються та з'являються нові шкідливі загрози. У цифровому світі, який постійно змінюється, мережна безпека ще ніколи не була такою важливою.

Мережні атаки останніх років демонструють, що зловмисники можуть завдати удару в найменш очікуваний момент. Саме тому, пильність і безпека мають бути пріоритетними для будь-яких інформаційних мереж.

Сьогодні на ринку безпеки існує велика кількість різноманітних засобів захисту мереж. Серед цих засобів особливої уваги заслуговують системи виявлення та запобігання вторгненням.

Рішення виявлення та запобігання вторгненням (IDS/IPS) діють превентивно, вони виявляють і запобігають несанкціонованим і потенційно зловмисним діям в інформаційних мережах. Запобігання вторгненням є критично важливим компонентом комплексної стратегії безпеки, оскільки воно блокує зловмисникам доступ до мережі та спричинення потенційно непоправних і дорогих збитків.

Дана кваліфікаційна робота присвячена дослідженню систем виявлення та запобігання вторгнень. Аналіз інформаційних джерел за тематикою роботи [1 – 28] підтвердив важливість та актуальність даного напрямку досліджень, саме тому ця кваліфікаційна робота є актуальною.

1 ЗАСОБИ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Згідно із Законодавством України, а саме в Законі України «Про електронні комунікації», безпека ІМ визначається так: безпека мереж і послуг – здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги [1].

В цілому, безпека інформаційної мережі забезпечується завдяки використанню стратегічного захисного підходу для обмеження будь-якого нелегального зовнішнього доступу шляхом забезпечення конфіденційності, цілісності та доступності даних, об'єктів і ресурсів мережі. Незалежно від розміру, кожна ІМ повинна мати процедури та інструменти для захисту від різних мережних загроз.

Безпека інформаційної мережі можлива при повноцінному захисті цифрової інфраструктури, програм, пристроїв та систем від онлайн-загроз. Цей захист охоплює безліч апаратних і програмних рішень і процесів, призначених для підтримки цілісності, конфіденційності та доступності інформаційних мереж.

1.1 Аналіз проблем безпеки в інформаційних мережах

Для того, щоб ефективно організувати безпеку інформаційних мереж перш за все необхідно виконати аналіз всіх можливих вразливостей та загроз безпеці ІМ. Послідовність взаємодії джерела загроз, вразливостей та наслідків [2] наведена на рис. 1.1. З рисунку видно, що при вчасному виявленні та нейтралізації джерел загроз та вразливостей можна уникнути реалізації загрози та не допустити негативні наслідки.

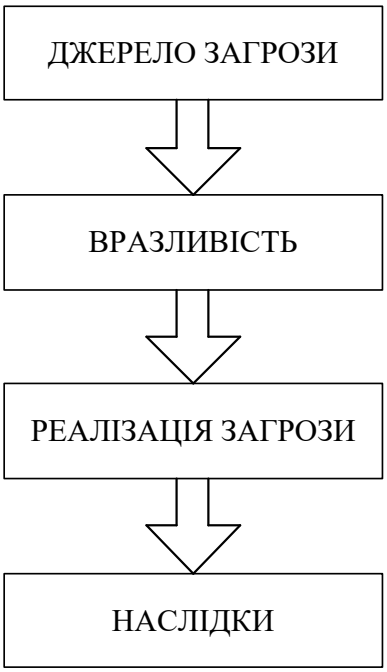

Рисунок 1.1 – Послідовність взаємодії джерела загроз, вразливостей та наслідків

На кожному етапі послідовності (рис. 1.1) вкрай важливо застосовувати всі можливі засоби безпеки. Ідентифікація можливих джерел загроз, виявлення та усунення вразливостей ІМ, попередження можливих реалізацій загроз – все це максимально захистить ІМ.

Загрози мережній безпеці – це потенційно можливі технологічні процеси, які послаблюють захист інформаційної мережі, ставлять під загрозу персональні дані, критичні програми та всю ІТ-інфраструктуру [3].

На сьогоднішній день існує велика кількість загроз (рис. 1.2), їх слід ретельно відстежувати та пом’якшувати найбільш критичні загрози та вразливості. Існує дві основні категорії загроз безпеки ІМ – випадкові та навмисні. Обидві категорії потребують ретельного аналізу та сучасних засобів боротьби проти них.

Особливу небезпеку представляють навмисні загрози – мережні атаки. Мережні атаки – це несанкціоновані дії з цифровими активами в інформаційній мережі. Зловмисники зазвичай здійснюють мережні атаки, щоб змінити,

знищити або викрасти персональні дані. Як правило, зловмисники під час мережних атак, націлюються на периметр мережі, щоб отримати доступ до внутрішніх систем [4].

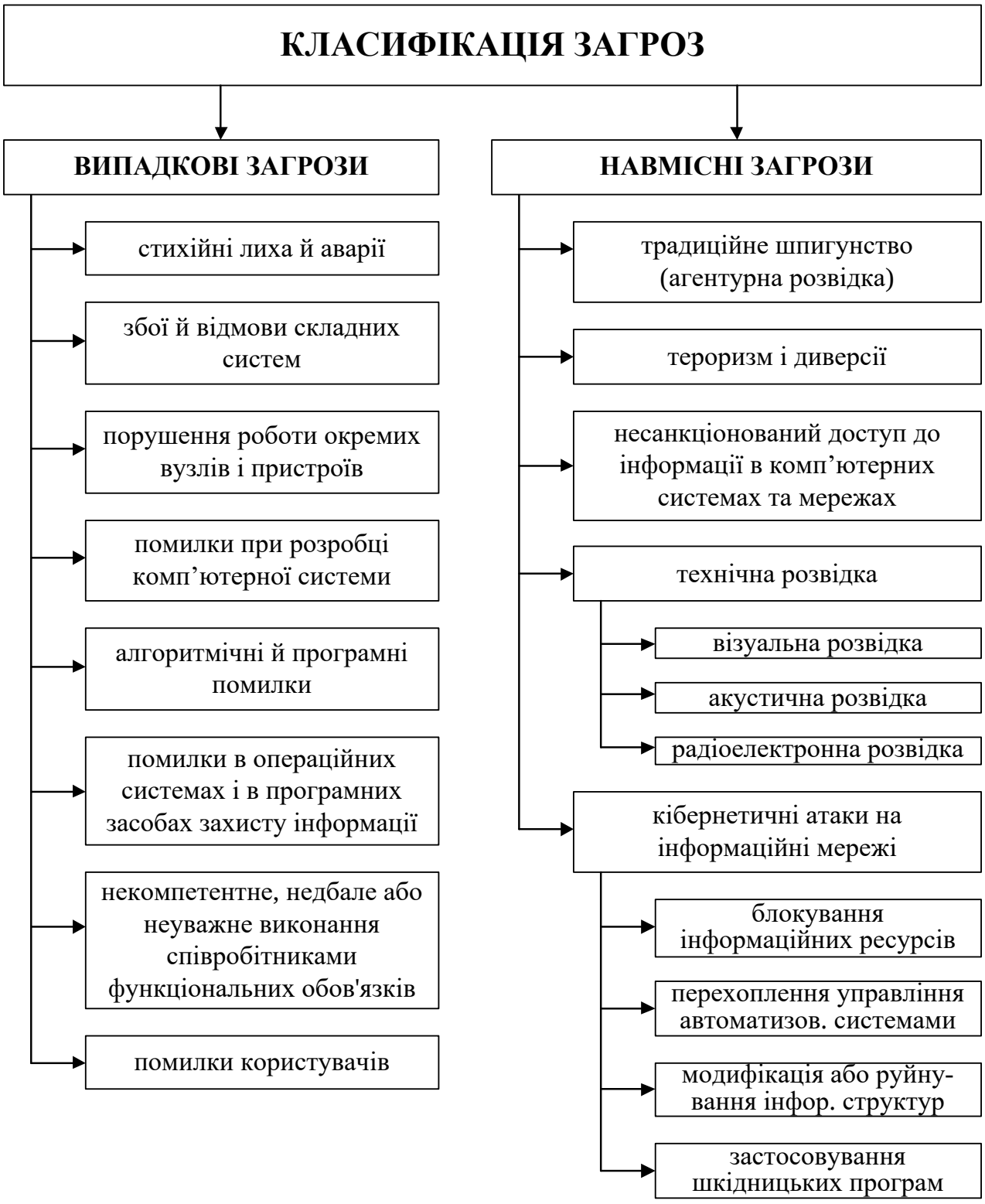

Рисунок 1.2 – Класифікація загроз ІМ

Існують пасивні та активні мережні атаки. При пасивних мережних атаках зловмисники отримують несанкціонований доступ до мереж, контролюють і викрадають персональні дані, не вносячи жодних змін. При активних мережних атаках зловмисники можуть змінювати, шифрувати або пошкоджувати інформацію та персональні дані. Сьогодні існує багато видів мережних атак, найбільш розповсюджені з них наведено на рис. 1.3.

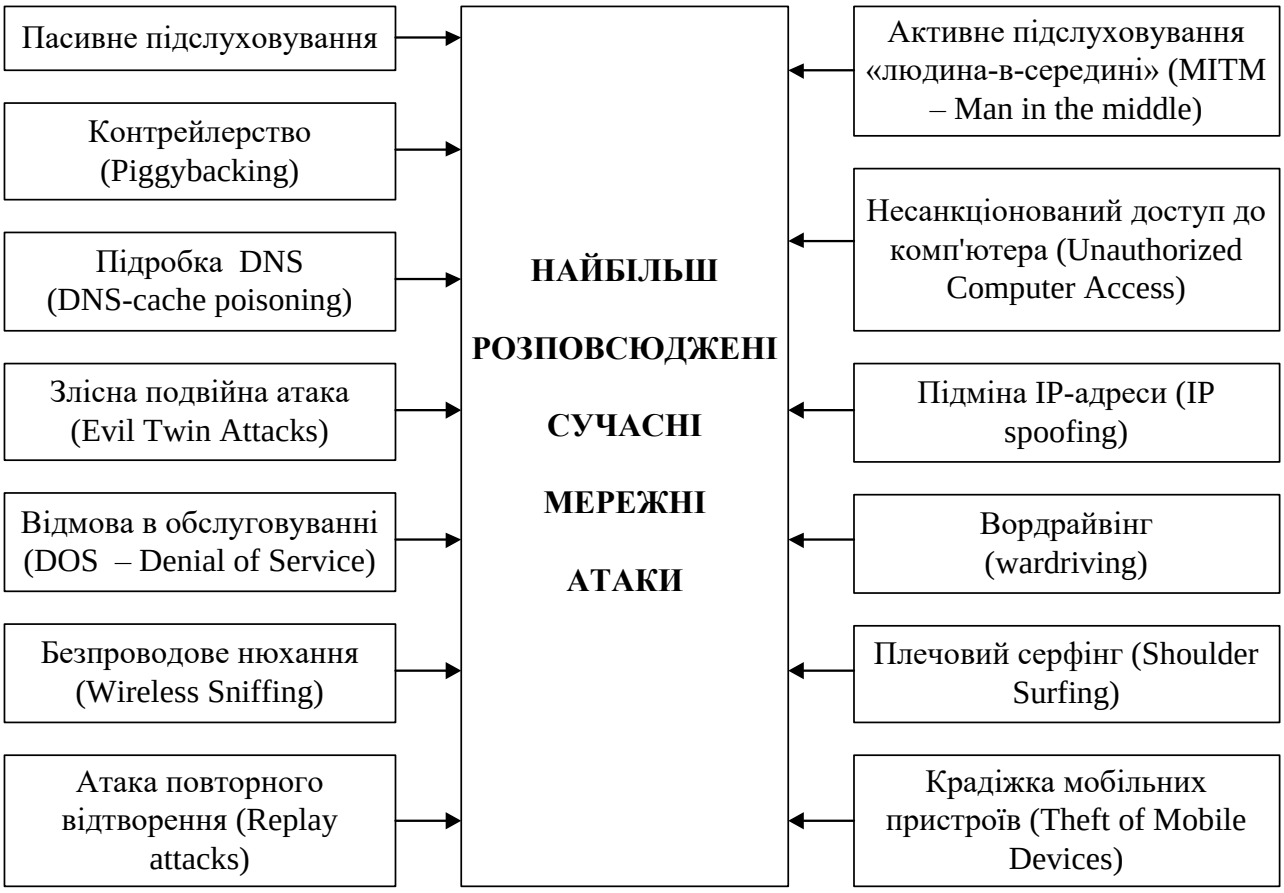

Рисунок 1.3 – Найбільш розповсюджені атаки на ІМ

Як правило, атаки та інші загрози мереженій безпеці спрямовані на використання вразливостей мережі для проникнення в ІМ та завдання шкоди конфіденційним даним, програмам і робочим навантаженням. Коли кіберзлочинець виявляє слабке місце в системі, він використовує його, щоб отримати несанкціонований доступ і встановити зловмисне, шпигунське або

інше шкідливе програмне забезпечення [5]. Вразливості мережі необхідно виявляти та нейтралізовувати.

Розуміння вразливостей мережі є критично важливим аспектом безпеки. Це стосується не лише визначення цих проблем; це передбачає глибоке розуміння їхніх потенційних наслідків і розробку ефективних контрзаходів. Важливість цього розуміння полягає в здатності мережі захищати конфіденційні дані, забезпечувати безперебійну роботу систем і захищати від порушень, які можуть мати значні наслідки [6].

Вразливості мережі стосуються слабких місць або недоліків у структурі, реалізації або роботі мережі, якими можуть скористатися кіберзловмисники. Зловмисники можуть використовувати вразливості, щоб отримати несанкціонований доступ, спричинити збої в мережі або викрасти дані. Основні вразливості сучасних інформаційних мереж наведено на рис.1.5.

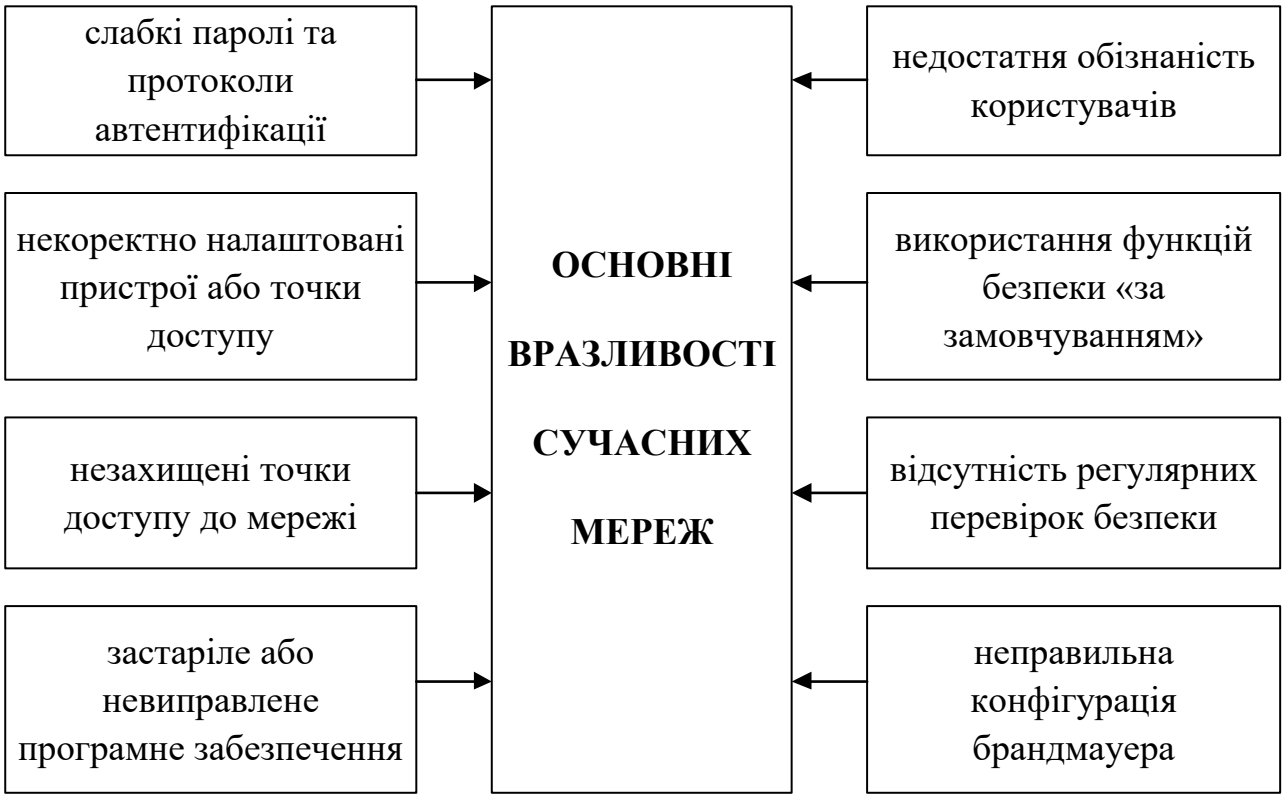

Рисунок 1.4 – Основні вразливості в ІМ

Прогалини в безпеці можуть виникати з різних джерел, зокрема застарілого програмного забезпечення, неправильно налаштованого апаратного забезпечення, слабких протоколів безпеки або людської помилки.

Застаріле програмне забезпечення становить значний ризик для безпеки через відомі вразливості, які часто усуваються в нових версіях. Таке програмне забезпечення не тільки не використовує останні функціональні вдосконалення, але й містить недоліки безпеки, які виявляються та потенційно використовуються кіберзлочинцями. Наявність цих вразливостей може створити низку проблем безпеки. Основною проблемою є неавторизований доступ, коли зловмисники використовують слабкі місця для проникнення в мережні системи. Порушення даних є ще одним серйозним ризиком, що призводить до потенційного викриття та крадіжки конфіденційної інформації [6]. Крім того, застаріле програмне забезпечення може стати каналом для зловмисного програмного забезпечення, дозволяючи шкідливому програмному забезпеченню проникати в мережу та компрометувати її. Загроза посилюється, коли відповідне програмне забезпечення є критичним для функціонування ключових систем або обробляє конфіденційні дані.

Значну загрозу безпеці становлять слабкі паролі. Легкий злом або можливість вгадати дозволяє зловмисникам отримати несанкціонований доступ. Ця вразливість посилюється, коли однакові слабкі паролі використовуються в кількох облікових записах або системах. Подібним чином залежність від застарілих протоколів автентифікації створює певний набір проблем. Ці старі системи часто не мають розширених функцій безпеки, вбудованих у сучасні методи, наприклад шифрування або багатофакторну автентифікацію. Як наслідок, вони більш вразливі до перехоплення або обходу, що залишає мережні ресурси відкритими для несанкціонованого доступу.

Критичною вразливістю в безпеці мережі є неправильна конфігурація брандмауера, яка часто виникає через недогляд або відсутність спеціального розуміння унікальних вимог до мережі. Брандмауери служать основним бар’єром проти несанкціонованого доступу, і їх ефективність залежить від

точної конфігурації та своєчасних оновлень. Проблеми часто виникають через складні набори правил брандмауера, недостатнє розуміння програм, що працюють у мережі, або нехтування адаптацією брандмауера до нових загроз. Такі збої можуть призвести до відкритих мережних портів, розблокованих IP-адрес або роботи непотрібних служб, усе це створює значні вразливості. Наслідки неправильно налаштованого брандмауера значні та серйозні. Це може зробити мережу такою ж вразливою, ніби вона взагалі не мала захисту брандмауером. Ця вразливість призводить до технічних збоїв, несанкціонованого доступу та витоку даних і навіть може створити основу для масштабніших мережних атак [6].

Відсутність регулярних перевірок безпеки в стратегії мережної безпеки призводить до того, що можна не помітити нових вразливостей і потенційних загроз. Аудити безпеки є критично важливими для систематичної оцінки та покращення стану безпеки мережі. Вони передбачають комплексне вивчення політики безпеки, практик і засобів контролю, щоб забезпечити ефективний захист від поточних кіберзагроз. Регулярні перевірки безпеки допомагають виявити слабкі місця в мережній інфраструктурі, такі як невиправлене програмне забезпечення, неправильно налаштоване обладнання та неадекватні протоколи безпеки. Аудити також відіграють ключову роль в оцінці ефективності засобів контролю доступу, перевіряючи, чи мають лише авторизовані особи доступ до конфіденційних систем і даних. Крім того, вони оцінюють фізичну безпеку мережних компонентів і перевіряють можливості організації реагувати на інциденти, щоб забезпечити готовність у разі порушення.

Особливої уваги потребує питання аналізу найновіших загроз та новітніх ризиків (рис. 1.5). З розвитком інформаційних технологій, поширенням дистанційних бізнес-процесів, збільшення кількості користувачів та пристроїв, популяризацією концепції гібридної та віддаленої роботи перелік загроз постійно еволюціонує.

Велика кількість нових загроз безпеці, що розвиваються, тримає індустрію інформаційної безпеки у стані підвищеної готовності. Дедалі складніші кібератаки, пов’язані зі зловмисним програмним забезпеченням, фішингом, машинним навчанням і штучним інтелектом, криптовалютою тощо, піддають інформаційні мережі постійній небезпеці [7].

Рисунок 1.5 – Новітні ризики в ІМ

Окрім наведених на рис.1.5 найголовніших новітніх проблем безпеки, існує багато і інших, зокрема:

– фішинг стає все складнішим,

– швидко розвиваються стратегії програм-вимагачів,

– криптоджекінг (це новий тренд, у якому кіберзлочинці захоплюють сторонні домашні чи робочі комп’ютери з метою «майнінгу» криптовалюти),

– постійна загроза хакерських атак, націлених на критичну інфрастуктуру (електромережі, транспортні системи, водоочисні споруди тощо), є основною вразливістю майбутнього [7],

– збільшення атак спрямованих на державні системи,

– проблеми конфіденційності з підключеними автомобілями та напівавтономними транспортними засобами тощо.

Для того, щоб мінізувати негативний вплив цих новітніх ризиків та загроз, необхідно завжди бути в курсі найновіших проблем безпеки, слідкувати за новинами в галузі кібербезпеки та своєчасно реагувати на можливі потенційні загрози та застосовувати найновіші засоби безпеки.

1.2 Інструменти мережної безпеки

Розвиток мережних атак потребує сучасного та проактивного рішення для захисту інформаційних мереж, що надаватиме набір актуальних складних функцій, необхідних для виявлення та реагування на найпідступніші загрози в мережі.

Інструменти мережної безпеки (рис. 1.6) – це різноманітні технічні, апаратні або програмні засоби, які створюються спеціально для забезпечення безпеки інформаційної мережі та застосовують такі методи, як моніторинг, перевірка з’єднань та сповіщення.

Інструменти безпеки електронної пошти необхідні для виявлення небезпечних електронних листів, блокування фішингових та інших атак, запобігання витоку інформації.

Інструменти контролю доступу необхідні для контролю легального доступу, ведення баз даних користувачів і управління адміністративними інструментами для політики контролю доступу, аудиту та примусового виконання.

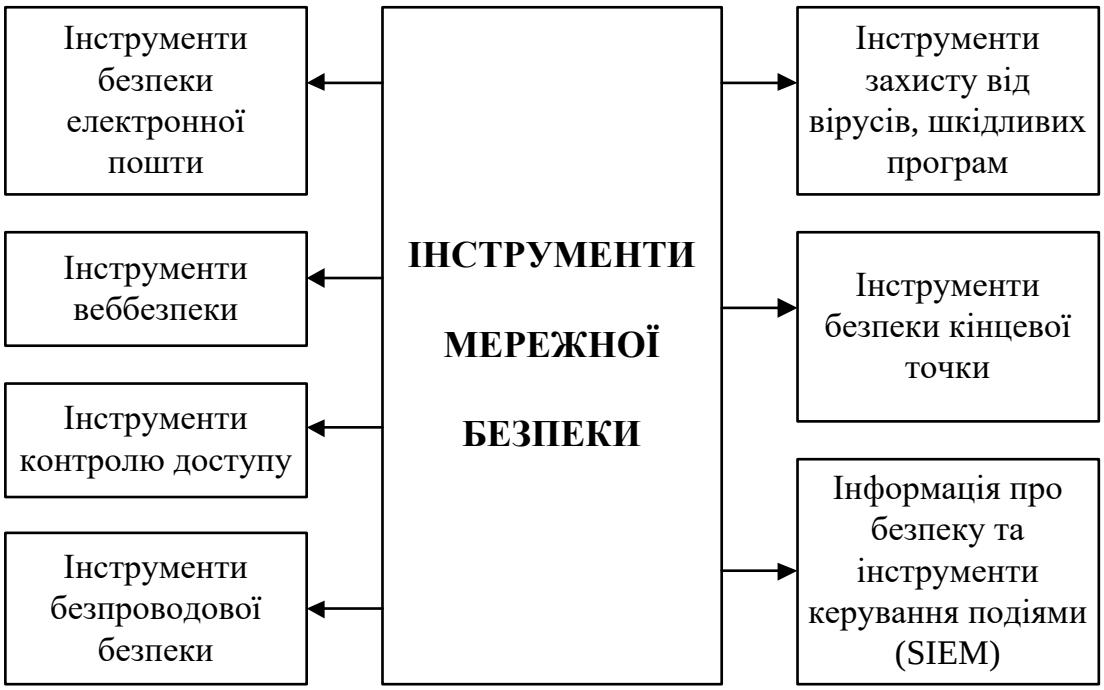

Рисунок 1.6 – Основні категорії інструментів мережної безпеки

Інструменти веббезпеки необхідні для періодичного сканування вебсайтів з метою виявлення небезпечних дій або загроз безпеці.

Інструменти захисту від вірусів і шкідливих – це тип програмного забезпечення безпеки ІМ, що необхідні для виявлення та нейтралізації шкідливих програм, виправлення зараження небезпечним ПЗ і мінімізації шкоди для мережі.

Інструменти керування подіями (Security Information and Event Management Tools, SIEM) необхідні для виявленяи, аналізу та реагування на загрози безпеці до того, як вони вплинуть на роботу мережі [8].

Інструменти безпеки кінцевої точки необхідні для відстеження, моніторингу та керування набором кінцевих пристроїв, що використовуються в інформаційній мережі.

Засоби мережної безпеки – це програмні та апаратні засоби, призначені для захисту ІМ від несанкціонованого доступу, атак і зловмисного ПЗ. Вони використовують передові технології та методи для захисту та моніторингу

мережі та запобігання зловмисним діям [9]. Деякі найпопулярніші засоби безпеки мереж представлено на рис. 1.7.

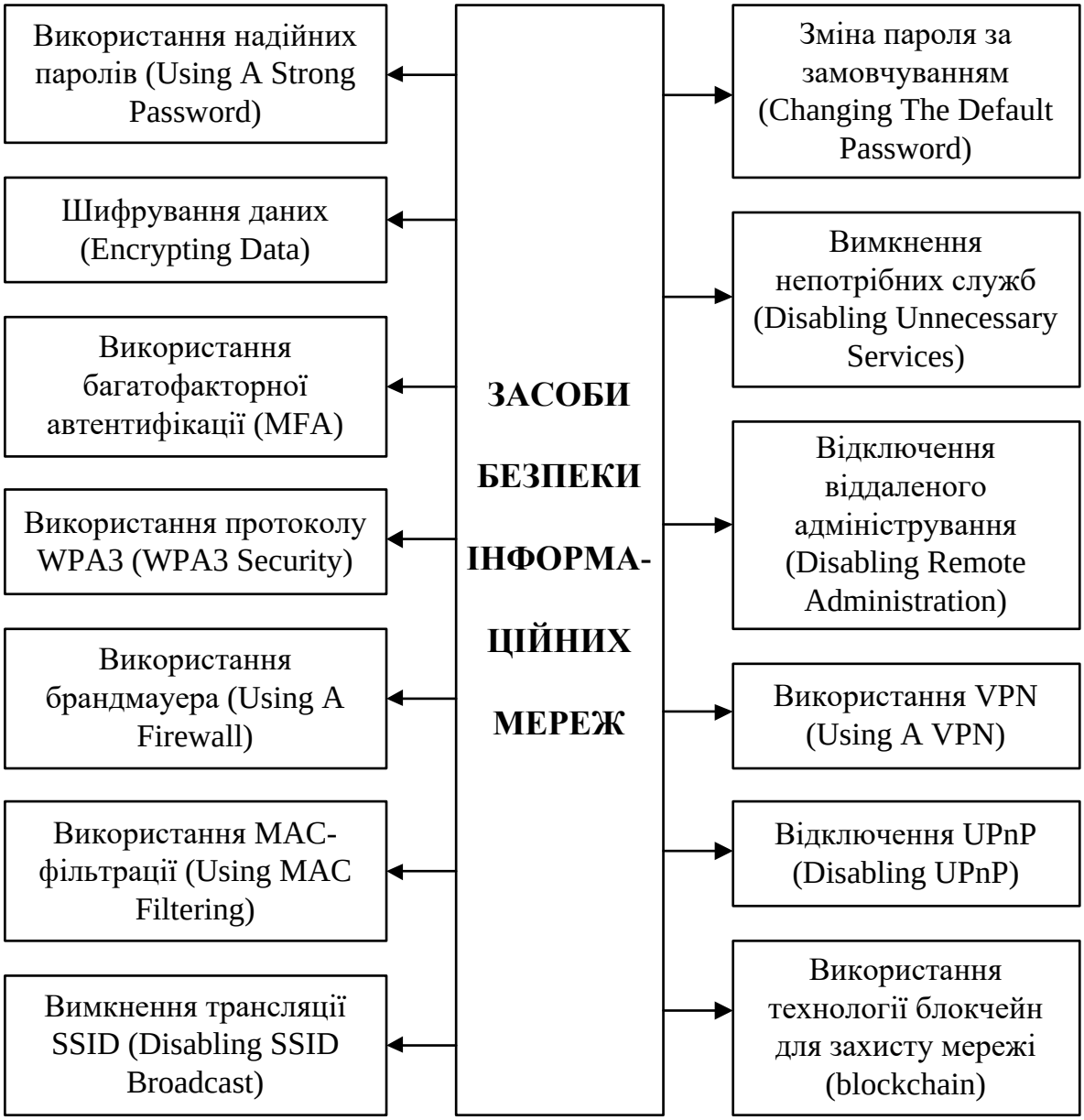

Рисунок 1.7 – Найпопулярніші засоби безпеки ІМ

Брандмауери – це інструменти безпеки мережі, які діють як бар’єр між внутрішньою мережею та зовнішнім інтернетом. Вони працюють, фільтруючи вхідний і вихідний трафік і блокуючи будь-які неавторизовані або підозрілі пакети даних. Брандмауери забезпечують додатковий рівень безпеки мережі та допомагають запобігти витоку даних.

Антивірусне програмне забезпечення призначене для захисту мережі від вірусів, зловмисного програмного забезпечення та іншого шкідливого програмного забезпечення шляхом сканування файлів, електронних листів та інших даних на наявність потенційних загроз і попередженя користувачів при їх виявленні.

Системи виявлення та запобігання вторгненням (Intrusion detection system /Intrusion prevention system, IDS/IPS) призначені для моніторингу мережного трафіку та виявлення будь-якої підозрілої активності. IDS/IPS працюють, аналізуючи шаблони мережного трафіку та сповіщаючи адміністраторів мережі, якщо виявляють будь-які незвичні дії, які можуть вказувати на спробу кібератаки. Системи IPS також мають можливість запобігати атакам, блокуючи зловмисний трафік.

Віртуальні приватні мережі (VPN) – це зашифроване мережне з’єднання, яке дозволяє безпечно передавати дані через інтернет. VPN є корисними інструментами безпеки мережі для віддалених працівників або дистанційної роботи, яким потрібен безпечний доступ до ресурсів компанії поза межами офісної мережі [9].

Засобів безпеки сьогодні існує дуже багато, але особливої уваги заслуговують засоби виявлення вразливостей та запобігання вторгнень. Адже набагато ефективніше виявити та не допустити вторгнення, ніж боротися з наслідками шкідливих впливів.

1.3 Засоби виявлення та усунення вразливостей

Мета захисту ІМ полягає не стільки в тому, щоб реагувати на інциденти, скільки в тому, щоб запобігати їм, забезпечуючи безпеку та цілісність мереж і цінних даних, які вони містять.

У безпеці мережі життєво важливі пильність і профілактичні заходи. Розпізнавання та усунення вразливостей мережі – це не одноразове завдання, а постійний процес, який вимагає постійної уваги та адаптації.

Управління вразливістю – це системний підхід до керування слабкими місцями безпеки, який стоїть на першому місці ефективної стратегії кібербезпеки [10].

Управління вразливістю є безперервним циклом, який включає кілька ключових етапів (рис. 1.8).

Рисунок 1.8 – Процес управління вразливостями

Виявлення вразливостей виконується за допомогою автоматизованих засобів сканування та ручного тестування. Автоматичне сканування виконується через мережу за допомогою локальних агентів у системах, а ручне тестування виконується зазвичай за допомогою тестуванням на проникнення.

Оцінка серйозності та потенційного впливу виявлених вразливостей повинна брати до уваги технічний захист, архітектуру системи та потенційний вплив. Цей етап виконують досвідчені аналітики.

Пріоритезація – це визначення вразливостей, які потрібно усунути в першу чергу, на основі їх рівня ризику. Огляд усіх вразливостей та їх рівнів ризику (серйозність і вплив) та доступні ресурси (час, люди, гроші) визначають пріоритетність вразливостей для усунення.

Ремедіація – це впровадження заходів для пом’якшення або усунення вразливостей [10].

Верифікація – це підтвердження успішного усунення вразливостей. Зазвичай виконується під час наступного автоматичного сканування, це важливий крок у мінімізації помилкового відчуття безпеки. Однак у випадках, які спочатку передбачали ручне тестування, слід провести додаткове ручне тестування [10].

Документація – це ведення детальних записів про вразливості та дії з їх усунення для цілей відповідності та аудиту.

Основним етапом процесу управління вразливостями є етап виявлення вразливостей. Засоби виявлення вразливостей наведені на рис. 1.9.

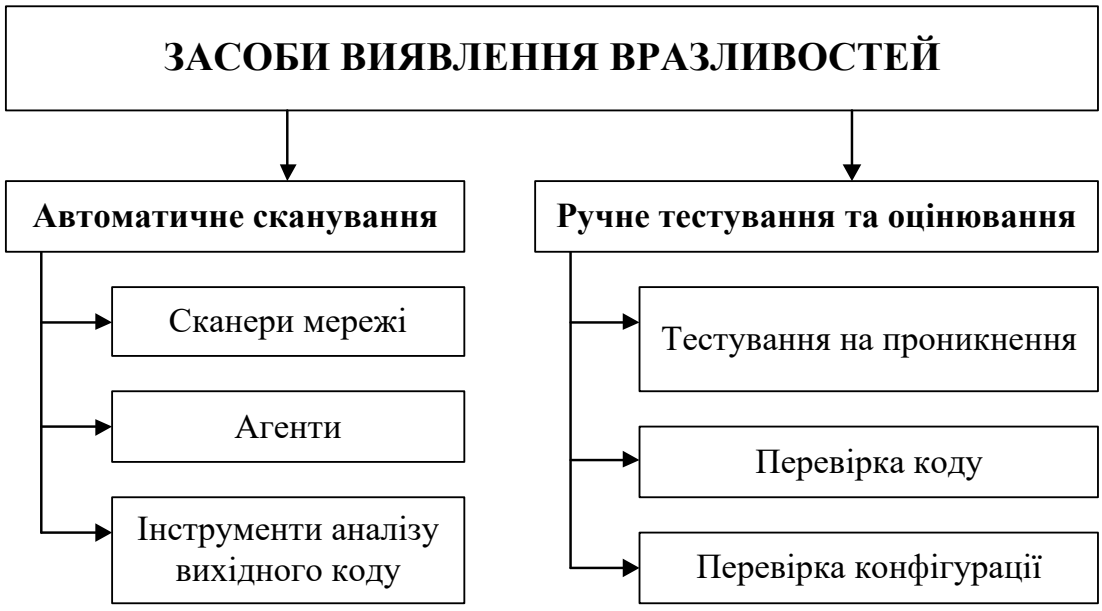

Рисунок 1.9 – Засоби виявлення вразливостей

Інструменти автоматичного сканування використовуються для керування вразливими місцями, вони є масштабованим і ефективним методом виявлення вразливостей у великих інформаційних мережах.

Сканери мережі сканують мережу на наявність пристроїв і виявляють вразливі місця в їх конфігураціях і доступних службах. Деякі з них зосереджені на слабких місцях безпеки веб-додатків, таких як впровадження SQL або вразливості міжсайтових сценаріїв.

Агенти, встановлені на клієнтах і серверах, аналізують те, що запущено та встановлено на пристрої, а потім порівнюють його з відомими вразливими місцями.

Інструменти аналізу вихідного коду або статичного тестування безпеки програми (SAST) шукають уразливості у вихідному коді та сховищах вихідного коду.

Вибір правильної комбінації цих інструментів залежить від конкретної інфраструктури та типів програм, що використовуються. Регулярне використання цих інструментів у поєднанні з оновленнями та налаштуваннями формує основу ефективної стратегії виявлення.

Хоча автоматизовані інструменти можуть ідентифікувати широкий спектр вразливостей, вони можуть виявити не все. Тому ручне тестування, яке часто виконується кваліфікованими тестувальниками проникнення, відіграє вирішальну роль у комплексній програмі виявлення вразливостей.

Тестування на проникнення (пентестування) – етичні хакери моделюють кібератаки, щоб перевірити стійкість систем і виявити вразливі місця, які автоматизовані інструменти можуть пропустити.

Для додатків експерти з безпеки можуть проводити перевірку вихідного коду вручну, щоб виявити недоліки безпеки, які автоматизовані інструменти не здатні виявити.

Перевірка конфігурацій системи та архітектури мережі вручну може виявити неправильні конфігурації або порушення політики, які можуть призвести до вразливостей.

Поєднання автоматизованих інструментів із ручним тестуванням дає повніше уявлення про безпеку і дає змогу виявляти як типові вразливості, так і складні проблеми безпеки, для визначення яких потрібен людський досвід [10].

На особливу увагу сьогодні заслуговує пентестування. Метою тесту на проникнення є методична перевірка безпеки системи з використанням усіх методів і стратегій, які використовують зловмисники. Цей тип аудиту базується на ряді стандартів безпеки. Пентест базується на шестиетапній методології, яка являє собою ітеративний процес (рис. 1.10).

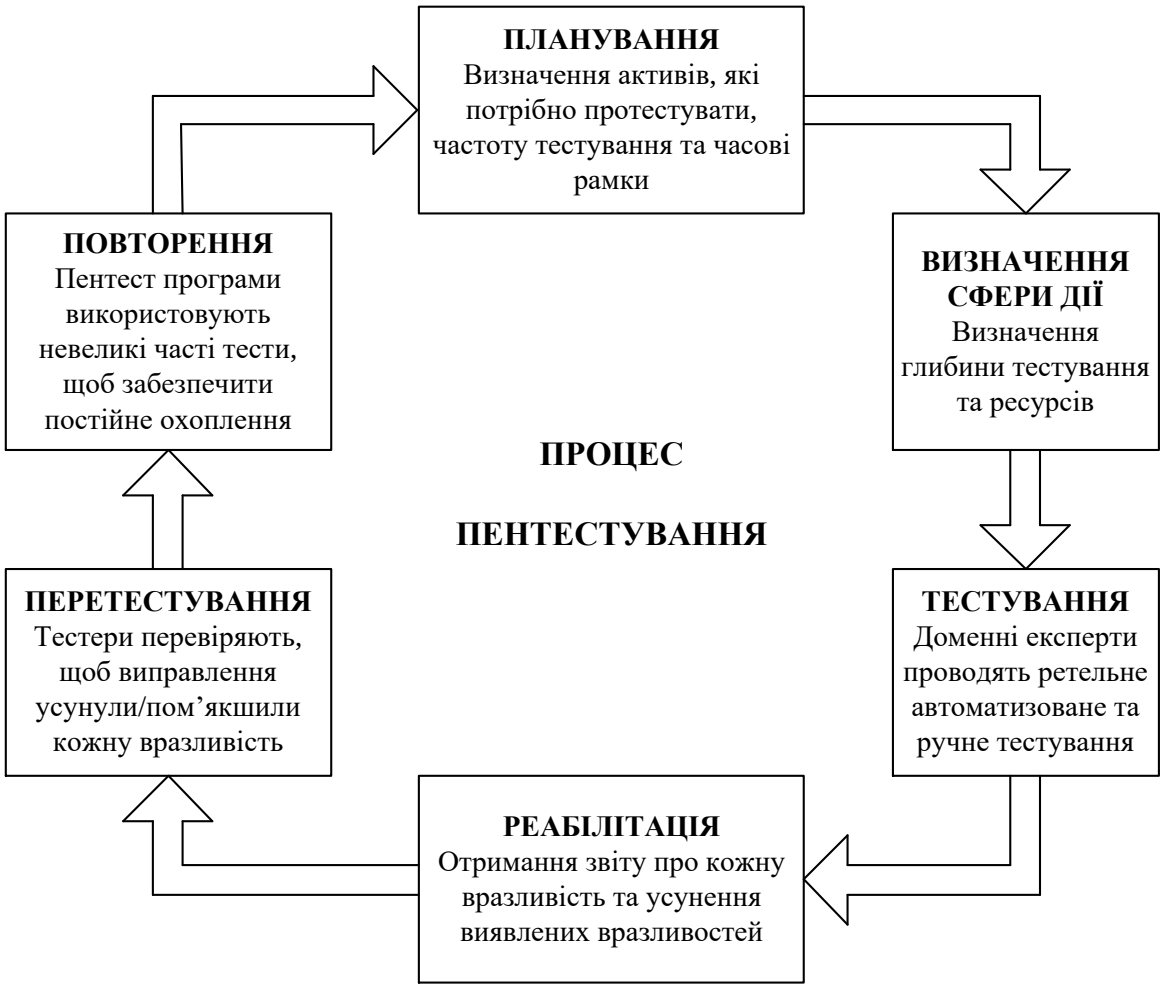

Рисунок 1.10 – Етапи пентестування

Тест на проникнення складається з ретельного дослідження конкретної цілі з метою виявлення найбільш критичних уразливостей. Результатом тесту

на проникнення є повний звіт, у якому представлені всі виявлені вразливості (класифіковані за рівнем критичності: низький, середній, високий, критичний), можливі експлойти та рекомендації щодо виправлення [11]. Пентестування має ряд переваг, що наведено на рис. 1.11.

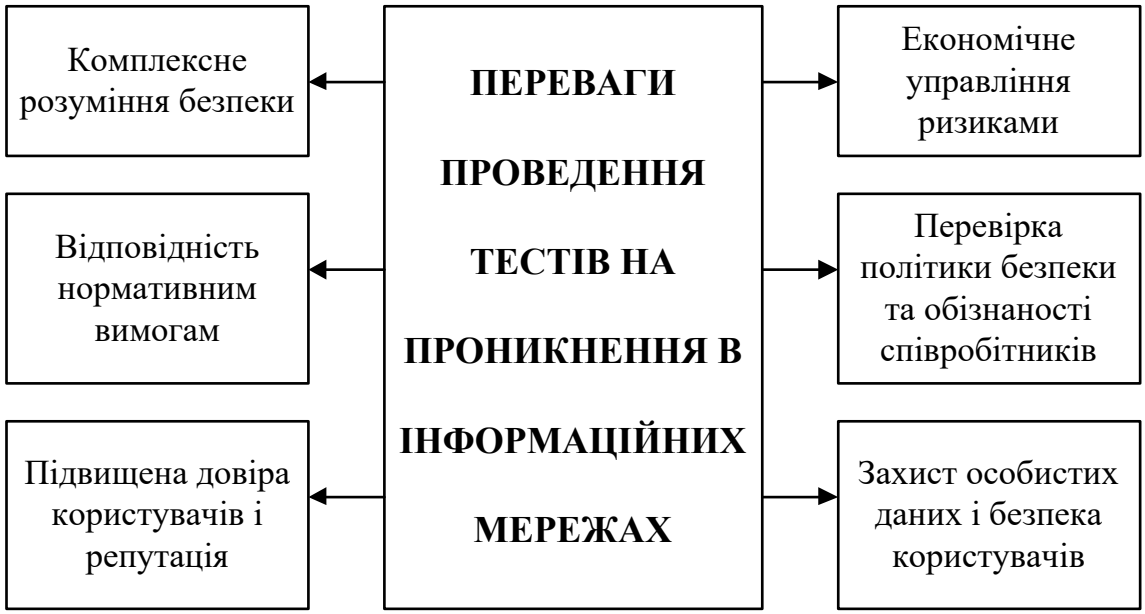

Рисунок 1.11 – Переваги пентестування

Тест на проникнення є спробою оцінити безпеку ІМ шляхом безпечного використання вразливостей. За допомогою тестування на проникнення можна завчасно виявити слабкі місця безпеки, які найбільше використовуються, перш ніж це зробить хтось інший.

Таким чином, успішне управління вразливостями вимагає постійних зусиль і уваги, щоб адаптуватися до нових загроз і вразливостей.

1.4 Засоби виявлення та запобігання вторгнень

До засобів виявлення та запобігання вторгнень відносяться брандмауери та системи виявлення/запобігання вторгнень (IDS/IPS). В наш час, коли кіберзагрози постійно розвиваються, брандмауери та IDS/IPS служать

охоронцями безпеки мережі. Ці критично важливі інструменти не тільки діють як бар’єри проти несанкціонованого доступу, але й забезпечують інтелектуальні дані, необхідні для виявлення потенційних вторгнень і реагування на них.

Основна мета брандмауера полягає в тому, щоб визначити, чи запити, видані одним обчислювальним пристроєм для ініціювання з’єднання з іншим пристроєм, повинні бути дозволені чи ні на основі правил, налаштованих адміністратором брандмауера. Існує два типи брандмауерів:

– персональні брандмауери на основі програмного забезпечення, які в основному є розширеннями операційної системи робочої станції,

– мережні брандмауери, які є апаратними пристроями, які фізично пропускають трафік за допомогою тих самих механізмів, що й мережні маршрутизатори та комутатори [12].

Брандмауер є основним рішенням для запобігання надходженню небажаного та підозрілого трафіку до системи. Брандмауер регулює те, що потрапляє в мережу, IDS/IPS регулює те, що проходить через систему. IDS/IPS часто знаходиться прямо за брандмауерам, працюючи в тандемі.

Система виявлення вторгнень (IDS) – це програмне забезпечення, яке можна встановити на фізичному чи віртуальному сервері або попередньо запрограмований пристрій, який перевіряє весь мережний трафік, що проходить через нього або через один або кілька комутаторів, до яких IDS підключено таким чином, що дозволяє переглядати трафік. IDS шукає мережний трафік підозрілого характеру. Подібно до програмного забезпечення для захисту від вірусів і шкідливих програм, IDS покладається на файл шаблонів шкідливого трафіку або сигнатур, які зберігаються в IDS і автоматично оновлюються на регулярній основі, зазвичай щодня. IDS може виявити постійні атаки, наприклад, атаки грубої сили (тобто повторні спроби входу на цільовий пристрій, щоразу вводячи інший пароль) і атаки зондування (тобто спроби перевірити, чи працює служба на будь-яких пристроях у мережі, якщо система має вразливості).

Система запобігання вторгненням (IPS) на відміну від IDS, призначена для виявлення підозрілого мережного трафіку та повідомлення про нього, дозволяє адміністраторам визначати дії, які IPS може виконувати для кожного виявленого шаблону підозрілого мережного трафіку. Дії, які може виконувати IPS, полягають, в основному, в тому, щоб дозволити трафіку продовжуватись або відхилити трафік.

Функції IDS та IPS відрізняються від брандмауерів тим, що брандмауери приймають рішення про дозвіл або блокування трафіку на основі IP-адреси джерела, IP-адреси призначення та запитаної послуги в кожному мережному пакеті. Пристрої IDS та IPS переважно приймають рішення на основі вмісту повідомлення, хоча IP-адреси та порти джерела та призначення можуть фігурувати в рівнянні [12].

Завдяки значним покращенням швидкості обробки комп’ютера, обсягу пам’яті та простору для зберігання, брандмауери останнього покоління тепер об’єднують деякі або всі наступні функції в одне інтегроване рішення: брандмауер, IDS/IPS, антивірус/захист від шкідливих програм, фільтрація спаму та VPN.

Стратегічне впровадження брандмауерів і систем виявлення вторгнень не підлягає обговоренню в пошуках надійної безпеки мережі. Розуміючи їхні можливості, старанно підтримуючи їх і використовуючи передові стратегії, адаптовані до унікальних потреб конкретної ІМ, можна значно покращити захист ІМ.

2 СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕННЯМ

2.1 Функціонал систем IDS/IPS

Система виявлення та запобігання вторгненням (IDS/IPS) визначається як система, яка відстежує мережу та сканує її на наявність можливих загроз, щоб попередити адміністратора та запобігти потенційним атакам [13].

IDS/IPS складається з двох систем: IDS та IPS (рис. 2.1). Система виявлення вторгнень (IDS) – це система, що виявляє зловмисну активність та сповіщає про це адміністратора. Система запобігання вторгненням (IPS) – це інструмент безпеки мережі (апаратний пристрій або програмне забезпечення), який постійно відстежує мережу на наявність зловмисної активності та вживає заходів для її запобігання, зокрема повідомляє, блокує або видаляє її, коли вона відбувається. Порівняння IDS та IPS [14] наведено в табл.2.1.

Рисунок 2.1 – Функціонал IDS та IPS

Таблиця 2.1 – Порівняння систем IDS та IPS

Параметр	Система виявлення вторгнень (IDS)	Система запобігання вторгненням (IPS)
Тип системи	Пасивний (моніторинг та сповіщення)	Активний (контроль та автоматичний захист)
Принцип роботи	– Виявляє трафік у режимі реального часу, – шукає шаблони трафіку або ознаки атаки, – генерує сповіщення	– Перевіряє трафік у реальному часі, – шукає шаблони трафіку або ознаки атаки, – потім запобігає атакам при виявленні
Механізм виявлення	– Виявлення сигнатур (сигнатури, що захищають від експлойтів)	– Виявлення на основі статистичних аномалій, – Виявлення сигнатур (сигнатури, що захищають від експлойтів, або сигнатури, спрямовані на вразливість)
Розміщення	Поза смугою передачі даних	На лінії передачі даних
Реакція на аномалію	Надсилає тривогу / сповіщення про виявлення шкідливого трафіку	Видалення, попередження або очищення шкідливого трафіку
Вплив на продуктивність мережі	Не впливає на продуктивність мережі через нелінійне розгортання IDS	Уповільнює продуктивність мережі через затримку, спричинену вбудованою обробкою IPS
Переваги	Не блокує законний трафік, який інколи може блокувати система IPS	Автоматичне виявлення та запобігання шкідливого трафіку

Для того, щоб IPS міг блокувати будь-який трафік, він повинен спочатку виявити та перевірити трафік, що описує функціональні можливості IDS. Замість двох окремих пристроїв, які виконують дві окремі функції, доцільно об’єднати ці дві системи в один пристрій. Саме тому, виробники об’єднують ці дві технології разом для можливості мати в одному продукті переваги їхньої функціональності [14].

Основні функції системи IDS/IPS наведено на рис. 2.2.

Рисунок 2.2 – Основні функції системи IDS/IPS

IDS/IPS захищає технологічну інфраструктуру та конфіденційні дані. В наш час інформаційні системи з’єднані мережами та постійно обмінюються

різними типами інформації. Дані постійно перетікають через мережу, тому найпростіший спосіб атакувати систему або отримати доступ до неї – це сховатися в самих даних. Частина IDS є реактивною – вона попереджає експертів із безпеки про такі можливі інциденти. Частина IPS є проактивною – вона дозволяє командам безпеки пом'якшувати ці атаки, які можуть завдати фінансової та репутаційної шкоди [13].

IDS/IPS переглядає існуючу політику користувача та політику безпеки. Кожна організація, що керується безпекою, має власний набір політик користувача та політики доступу для своїх програм і систем. Ці політики значно зменшують площу атаки, надаючи доступ до критичних ресурсів лише кільком довіреним групам користувачів і системам. Постійний моніторинг за допомогою систем виявлення та запобігання вторгненням гарантує, що адміністратори одразу помітять будь-які прогалини в цих структурах політики. Це також дозволяє адміністраторам налаштовувати політики для перевірки максимальної безпеки та ефективності.

IDS/IPS збирає інформацію про мережні ресурси. IDS-IPS також дає групі безпеки можливість побачити трафік, що проходить через його мережі. Це допомагає відстежувати мережні ресурси, дозволяючи модифікувати систему в разі перевантаження трафіком або недостатнього використання серверів.

IDS/IPS допомагає відповідати нормативним вимогам. Всі ІМ, незалежно від галузевої вертикалі, піддаються все більшому регулюванню для забезпечення конфіденційності та безпеки даних споживачів. Переважно першим кроком до виконання цих повноважень є розгортання системи виявлення та запобігання вторгненням.

Сисема IDS/IPS працює шляхом сканування процесів на наявність шкідливих шаблонів, порівняння системних файлів і моніторингу поведінки користувачів і системних шаблонів. IPS використовує брандмауери веб-додатків і рішення для фільтрації трафіку для запобігання інцидентам [15].

2.2 Архітектура та принцип роботи IDS/IPS

Системи IDS/IPS необхідно використовувати для моніторингу інформаційних мереж на наявність активності, що викликає недовіру або підозри. IDS/IPS допомогають виявити та запобігти атакам до того, як вони завдадуть значної шкоди ІМ.

Основні компоненти архітектури системи виявлення та запобігання вторгненням у мережу представлено на рис. 2.3.

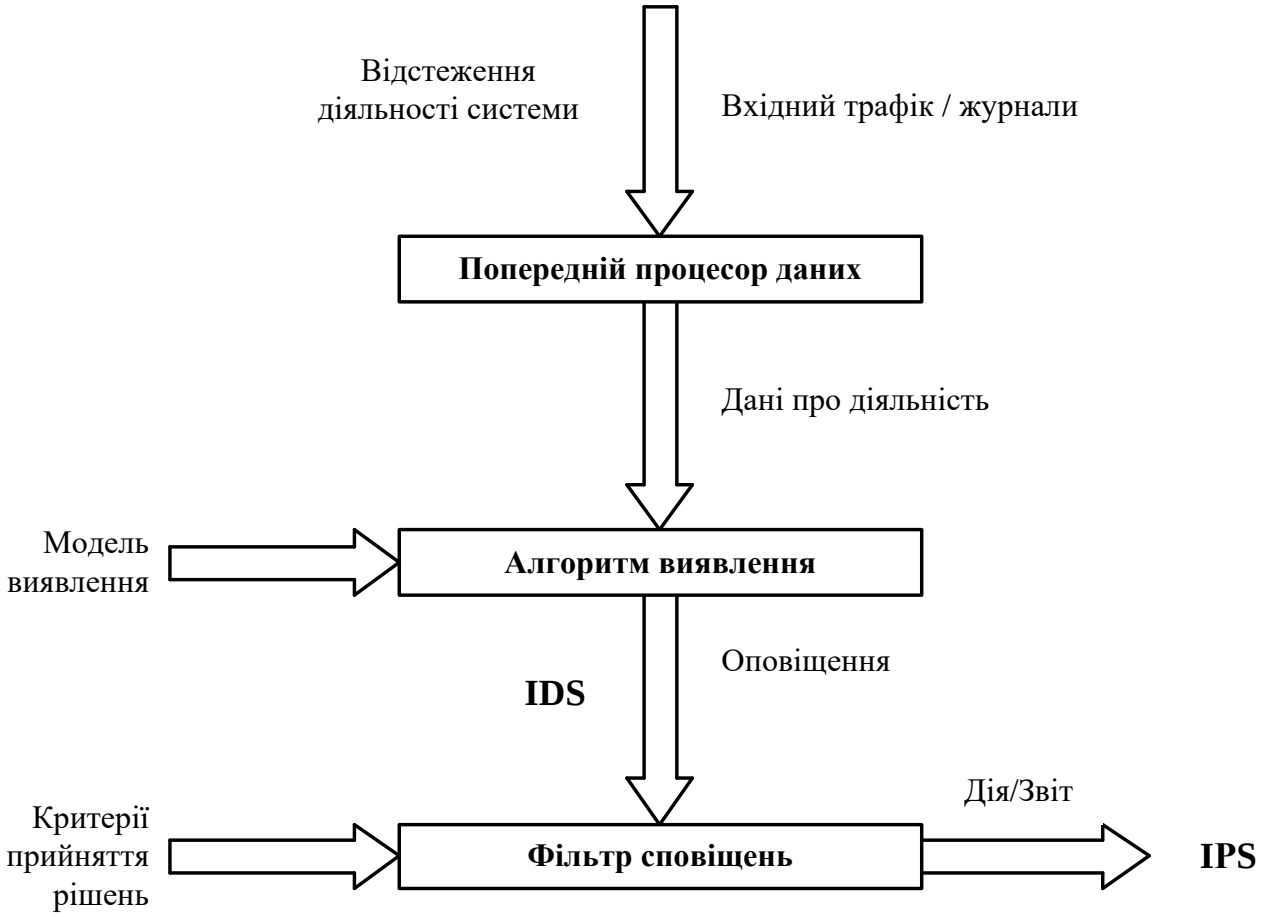

Рисунок 2.3 – Архітектура системи IDS/IPS

Система IDS/IPS складається з наступних компонентів: попередній процесор даних, алгоритм виявлення та фільтр сповіщень [16].

Попередній процесор даних відповідає за збір і форматування даних для аналізу за допомогою алгоритму виявлення вторгнень.

Алгоритм виявлення виявляє різницю між звичайним або законним і втручальним мережним трафіком на основі моделі виявлення.

Фільтр сповіщень оцінює ступінь серйозності вторгнення на основі критеріїв прийняття рішення та виявлених зловмисних дій. Потім фільтр сповіщень сповіщає мережного або системного адміністратора та виконує відповідні дії (зазвичай блокування).

IDS складається з алгоритму виявлення вторгнень і фільтра сповіщень, у якому попередньо визначено набори правил для виявлення загроз або вторгнень і створення даних про діяльність / журналів або сповіщень. IPS розгортається в мережі між мережними компонентами, щоб він міг вживати відповідних заходів проти зловмисної діяльності в мережі [16]. Він виконує такі ж дії моніторингу та аналізу, як і IDS, але не лише виявляє загрози чи вторгнення, але й вживає відповідних заходів щодо вторгнень, наприклад закриває з’єднання.

IDS визначає різницю між законним трафіком (дозволеними підключеннями) та спробою атаки на веб-сервер, порівнюючи сигнатуру веб-трафіку з базою даних відомих сигнатур атаки. IDS відіграє життєво важливу роль, повідомляючи адміністратора мережі про таку атаку та сповіщаючи його про вжиття відповідних заходів. З іншого боку, IPS відіграє життєво важливу роль, автоматично вживаючи відповідних дій під час спроби атаки. Наприклад, скидання / закриття з’єднання з веб-сервером. Таким чином, IDS діє пасивно, генеруючи журнали та сповіщаючи адміністратора мережі про спроби атаки або виникнення зловмисних дій, тоді як IPS активно відстежує такі дії та вживає заходів проти таких дій для захисту мережі. Таким чином, IDS і IPS діють як засоби захисту на рівні мережі для захисту інформаційної мережі [15].

Розміщення систем IDS і IPS в рамках інформаційної мережі показане на рис. 2.4.

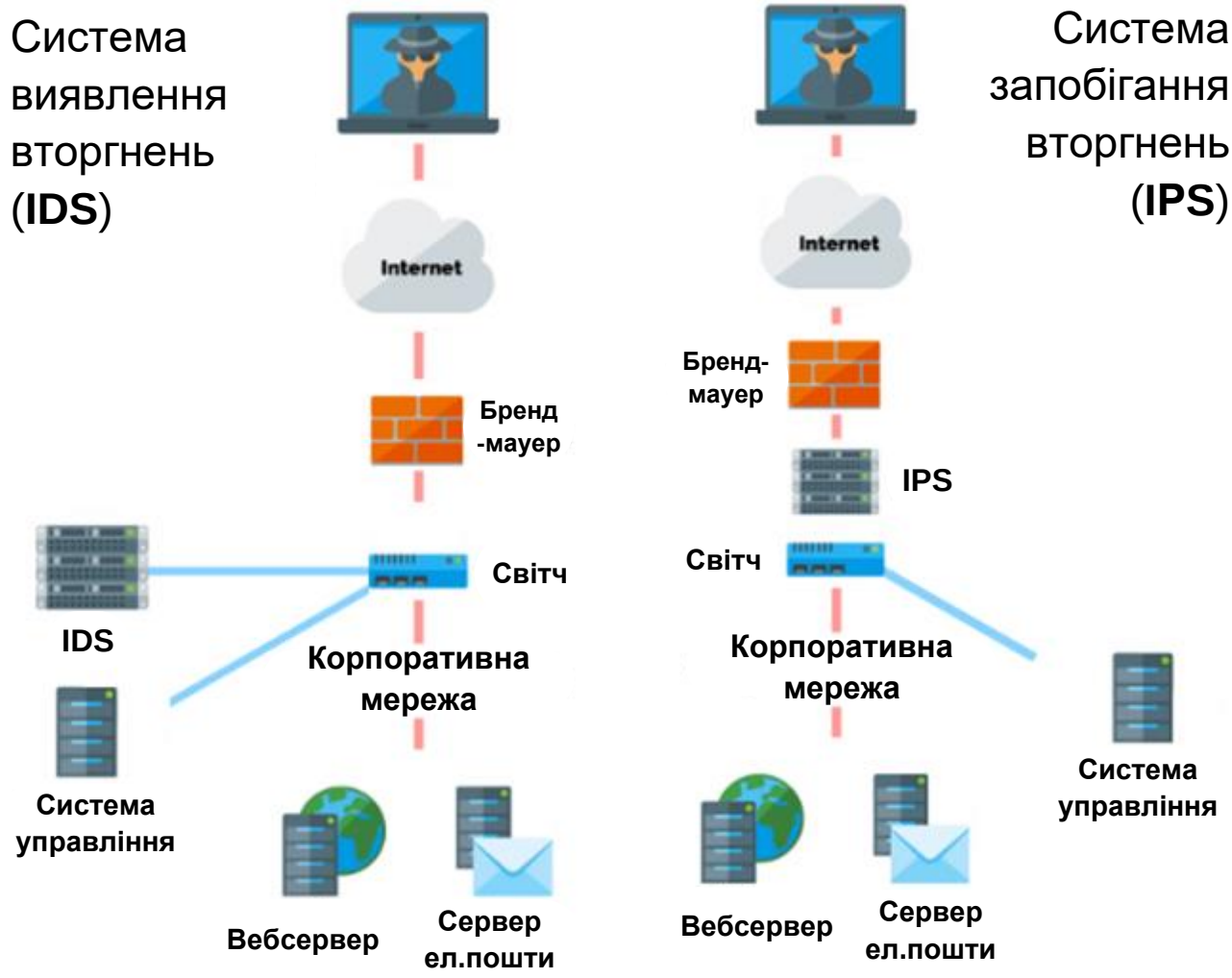

Рисунок 2.4 – Розміщення IDS та IPS в ІМ

IDS розміщується поза лінією мережного трафіку. На відміну від IDS, IPS розміщується в мережі одразу за брандмауером, на лінії прямого зв’язку між джерелом і отримувачем, активно аналізуючи та вживаючи автоматизованих дій щодо всіх потоків трафіку, які надходять у мережу [15].

Системи IDS/IPS поєднують корисність IDS та IPS із здатністю ефективно блокувати або пом’якшувати загрози. Рішення IDS/IPS можуть передаватися в режимі прямої дії, розташовуючись безпосередньо в межах активності, або поза смугою, де вони відображають дублікат активності. Вони можуть розрізняти небезпеки та реагувати на них природно, скорочуючи час реакції на потенційні атаки.

2.3 Класифікація систем IDS/IPS

Існує декілька типів рішень IDS/IPS [13, 17, 18], які використовуються для різних цілей. Тип системи IDS/IPS, необхідний конкретній компаніїї, залежить від її існуючої інфраструктури та планів її розширення в майбутньому. Важливим фактором також є техніка, яка використовуються рішеннями для виявлення та запобігання вторгненням. Класифікація систем IDS/IPS за призначенням наведена на рис. 2.5.

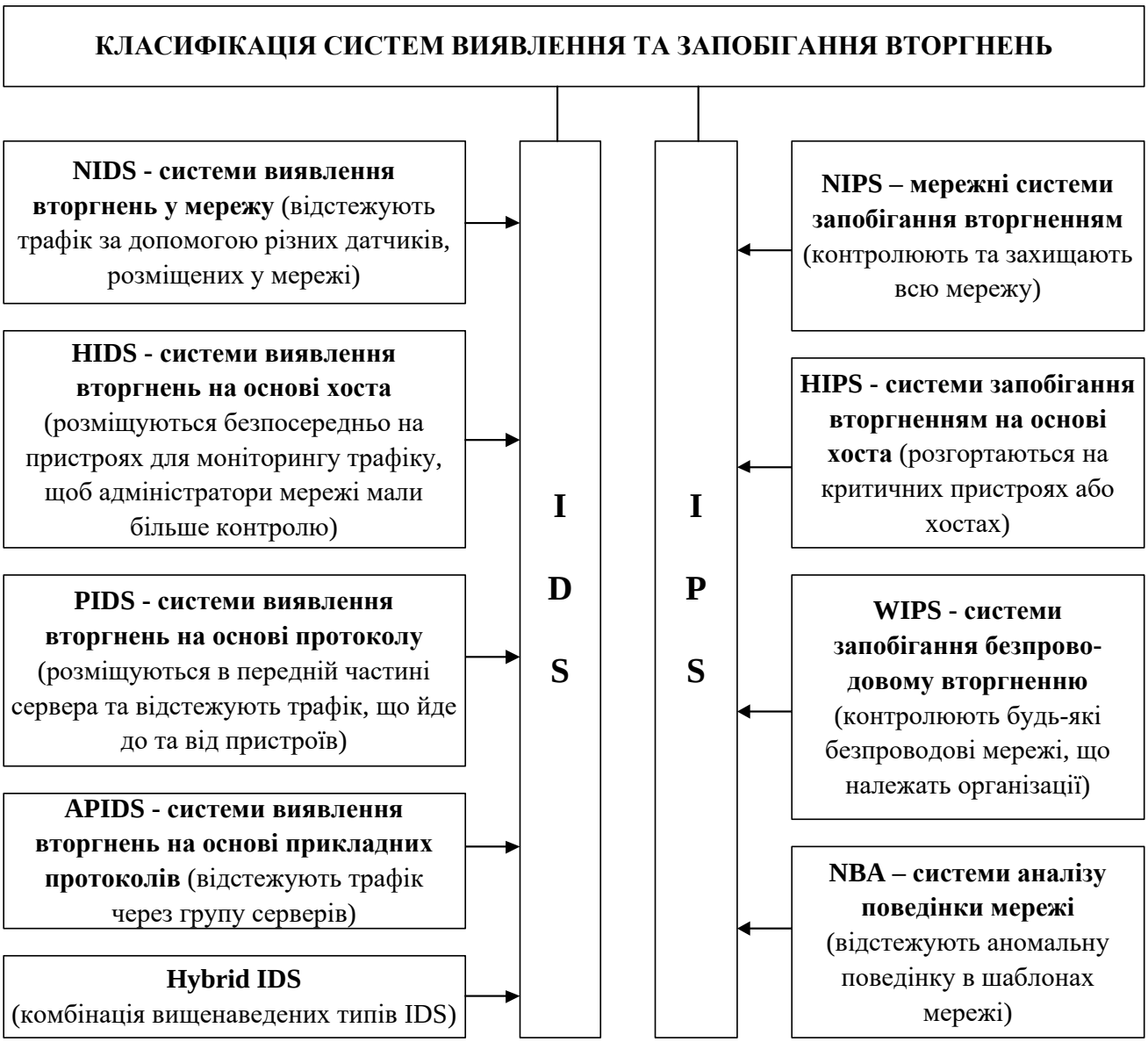

Рисунок 2.5 – Класифікація систем IDS/IPS

Мережні системи запобігання вторгненням (Network-based intrusion prevention system, NIPS) відстежують цілі мережі або сегменти мережі на наявність зловмисного трафіку. Зазвичай це робиться шляхом аналізу активності протоколу. Якщо активність протоколу збігається з базою даних відомих атак, відповідна інформація не може пройти. NIPS зазвичай розгортають на кордонах мережі, за брандмауерами, маршрутизаторами та серверами віддаленого доступу.

Системи запобігання безпроводовому вторгненню (Wireless intrusion prevention system, WIPS) відстежують безпроводові мережі, аналізуючи протоколи окремих безпроводових мереж. Хоча WIPS є цінним у діапазоні безпроводової мережі організації, ці системи не аналізують вищі мережні протоколи, такі як протокол керування передачею (TCP). Системи запобігання безпроводовому вторгненню розгортаються всередині безпроводової мережі та в зонах, чутливих до неавторизованого безпроводового підключення.

Системи аналізу поведінки мережі (Network behavior analysis system, NBA) визначають загрози, перевіряючи незвичні шаблони трафіку. Такі шаблони, як правило, є результатом порушень політики, атак, створених зловмисним програмним забезпеченням, або атак розподіленої відмови в обслуговуванні (DDoS). Системи NBA розгортаються у внутрішніх мережах організації та в точках, де трафік проходить між внутрішньою та зовнішньою мережами.

Системи запобігання вторгненням на основі хоста (Host-based intrusion prevention system, HIPS) відрізняються від інших тим, що вони розгорнуті на одному хості. Ці хости є критично важливими серверами з важливими даними або загальнодоступними серверами, які можуть стати шлюзами до внутрішніх систем. HIPS відстежує трафік, що надходить і виходить із цього конкретного хоста, відстежуючи запущені процеси, мережну активність, системні журнали, діяльність програми та зміни конфігурації.

Порівняння типів IPS [13] представлено в табл. 2.2.

Таблиця 2.2 - Порівняння типів систем IPS

Тип технології	Типи активності, що виявляє IPS	Область застосування	Перевага
NIPS	Діяльність мережного, транспортного та додаткового рівня TCP/IP	Кілька мережних підмереж і груп хостів	Тільки NIPS може аналізувати найширший діапазон прикладних протоколів
WIPS	Активність безпрово-дового протоколу; використання несанкціонованих безпроводових локальних мереж (WLAN)	Кілька WLAN і групи безпроводов их клієнтів	Тільки WIPS може передбачити активність безпроводового протоколу
NBA	Активність мережного, транспортного та додаткового рівня TCP/IP, яка спричиняє аномальні мережні потоки	Кілька мережних підмереж і груп хостів	NBA ефективніше, ніж інші, у виявленні розвідувального сканування та DoS-атак, а також у реконструкції основних заражень шкідливим програмним забезпеченням
HIPS	Хост-програма та діяльність операційної системи; мережний, транспортний та додатковий рівень TCP/IP	Індивідуаль-ні хости: критичні сервери або загально-доступні сервери	HIPS може аналізувати дії, передані під час наскрізного шифрування

Також системи виявлення та запобігання вторгнень класифікують за характером дії (рис. 2.6) та за методом виявлення вторгнень (рис. 2.7).

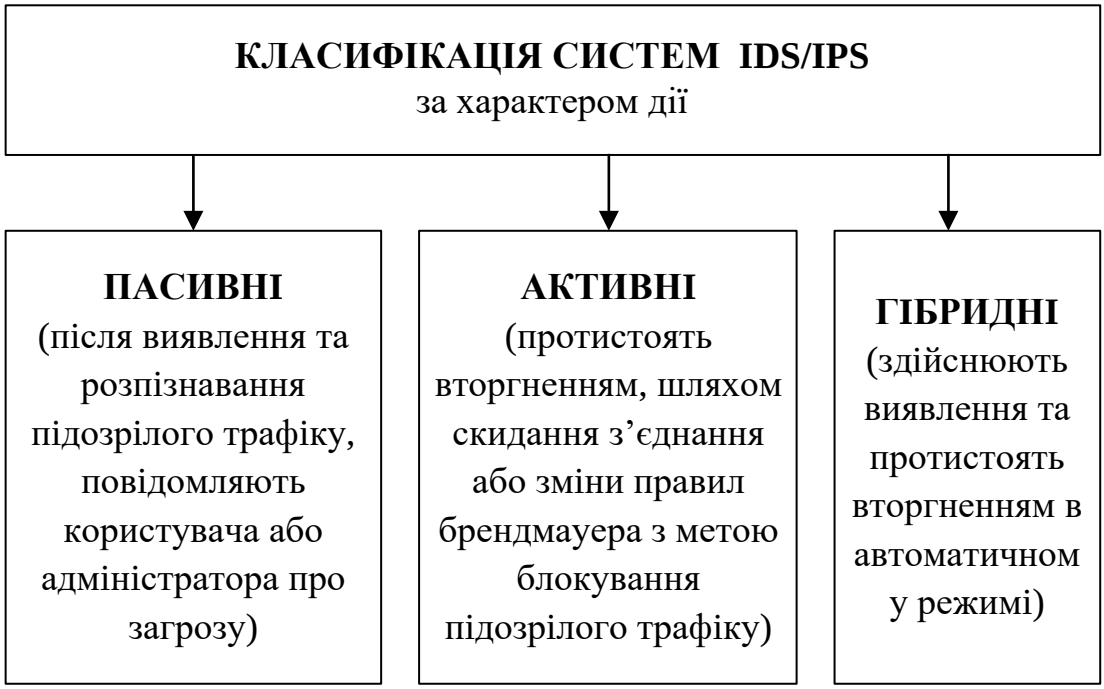

Рисунок 2.6 – Класифікація систем IDS/IPS за характером дії

Рисунок 2.7 – Класифікація систем IDS/IPS за методом виявлення вторгнень

За характером дії системи IDS/IPS бувають трьох типів: пасивні, активні та гібридні [17].

За методом виявлення вторгнень IDS/IPS бувать такі, що використовують для виявлення вторгнень сигнатури, аномалії або політики безпеки.

Метод виявлення на основі сигнатур зіставляє активність із сигнатурами відомих загроз. Система IDS/IPS підтримує базу даних сигнатур відомих зловмисних програм із виявленням на основі сигнатур. Щоразу, коли з'являється нове шкідливе програмне забезпечення, ця база даних оновлюється. Система виявлення працює, перевіряючи корисне навантаження трафіку за цією базою даних і сповіщаючи про збіг [13]. Одним із недоліків цього методу є те, що він може зупинити лише раніше ідентифіковані атаки та не зможе розпізнати нові.

Метод виявлення на основі аномалій відстежує аномальну поведінку шляхом порівняння випадкових зразків мережної активності з базовим стандартом. Виявлення аномалій працює над пороговим моніторингом і профілюванням. Налаштовано нормальну поведінку всіх користувачів, хостів, систем і програм. Будь-яке відхилення від цієї норми вважається аномалією і про нього попереджають. Виявлення аномалій краще, ніж виявлення на основі сигнатур, якщо розглядати нові атаки, яких немає в базі даних сигнатур. Створення цієї бази даних портебує багато часу. Навіть тоді показники помилкових спрацьовувань можуть бути високими, особливо в динамічному середовищі. Метод на основі аномалій більш надійний, ніж на основі сигнатур, але іноді може давати помилкові спрацьовування. Деякі новіші та вдосконалені системи запобігання вторгненням використовують штучний інтелект і технологію машинного навчання для підтримки моніторингу на основі аномалій.

Метод виявлення на основі політики менш поширений, ніж моніторинг на основі сигнатур або аномалій. Він використовує політики безпеки, визначені підприємством, і блокує дії, які порушують ці політики. Для цього потрібен адміністратор, щоб установити та налаштувати політики безпеки.

Кожен метод IDS/IPS має свої переваги та недоліки. Покладатися лише на один для захисту мережного трафіку недостатньо. Дійсно ефективна система виявлення та запобігання вторгненням використовує поєднання цих методів. При необхідності компанія може поєднати розгортання на основі мережі та хосту. Для кожного з них може знадобитися використовувати комбінацію методів виявлення сигнатур, аномалій і політик.

2.4 Переваги та недоліки IDS/IPS

Система IDS/IPS є ключовою частиною будь-якої корпоративної системи безпеки. Сучасні системи IDS/IPS мають багато переваг (рис. 2.8).

Сучасні системи IDS/IPS дозволяють визначати в реальному часі будь-які можливі слабкі місця в мережі для запобігання майбутнім атакам, оперативно виявляти вторгнення, зменувати ризик втрати даних через зловмисну діяльність або несанкціонований доступ.

IDS/IPS дозволяють захищати мережі від відомих і невідомих загроз, вразливостей, від зловмисного програмного забезпечення.

Висока видимість і детальний контроль інформаційної мережі в IDS/IPS дозволяє швидко виявляти й усувати будь-які потенційні загрози.

Можливість детального відстеження дій користувачів може визначити, чи беруть участь користувачі в підозрілих діях або демонструють зловмисну поведінку, яка може призвести до порушення безпеки.

Покращена відповідність різноманітним державним і галузевим нормам (напр. PCI DSS) і допомога компаніям відповідати цим нормам, надаючи додатковий рівень безпеки, дозволяє гарантувати, що всі дані захищені від несанкціонованого доступу.

IDS/IPS є економічно ефективними системами захисту, оскільки попереджують шкідливий вплив вторгнень, що є набагато дешевше вартість усунення наслідків порушення безпеки.

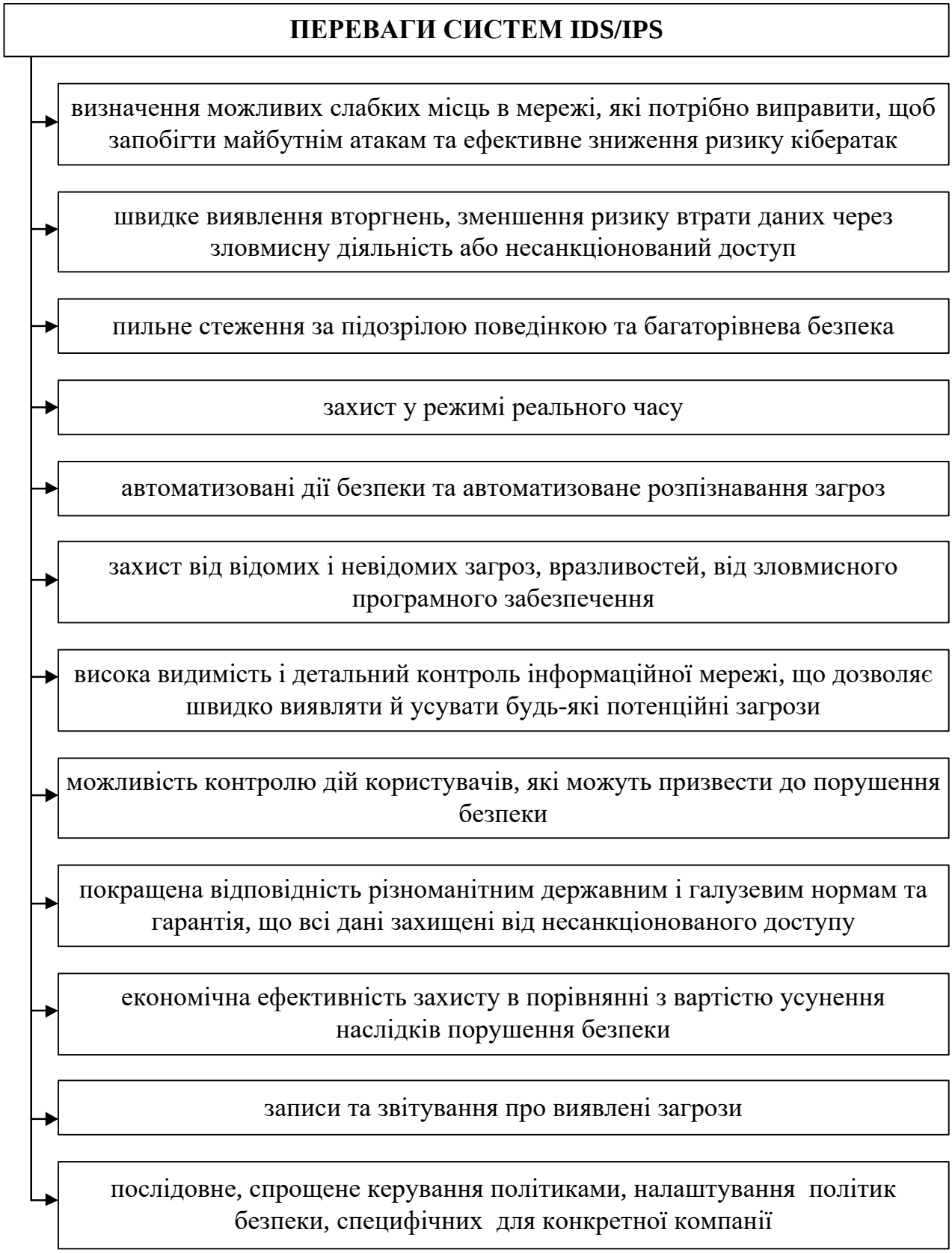

Рисунок 2.8 – Переваги систем IDS/IPS

Системи IDS/IPS також мають ряд недоліків (рис. 2.9). Недоліки систем виявлення та запобігання вторгненням детально проаналізовані та сформульовані в роботі [19], автори цієї роботи акцентують увагу на подальшому розвитку та вдосконаленні систем IDS/IPS.

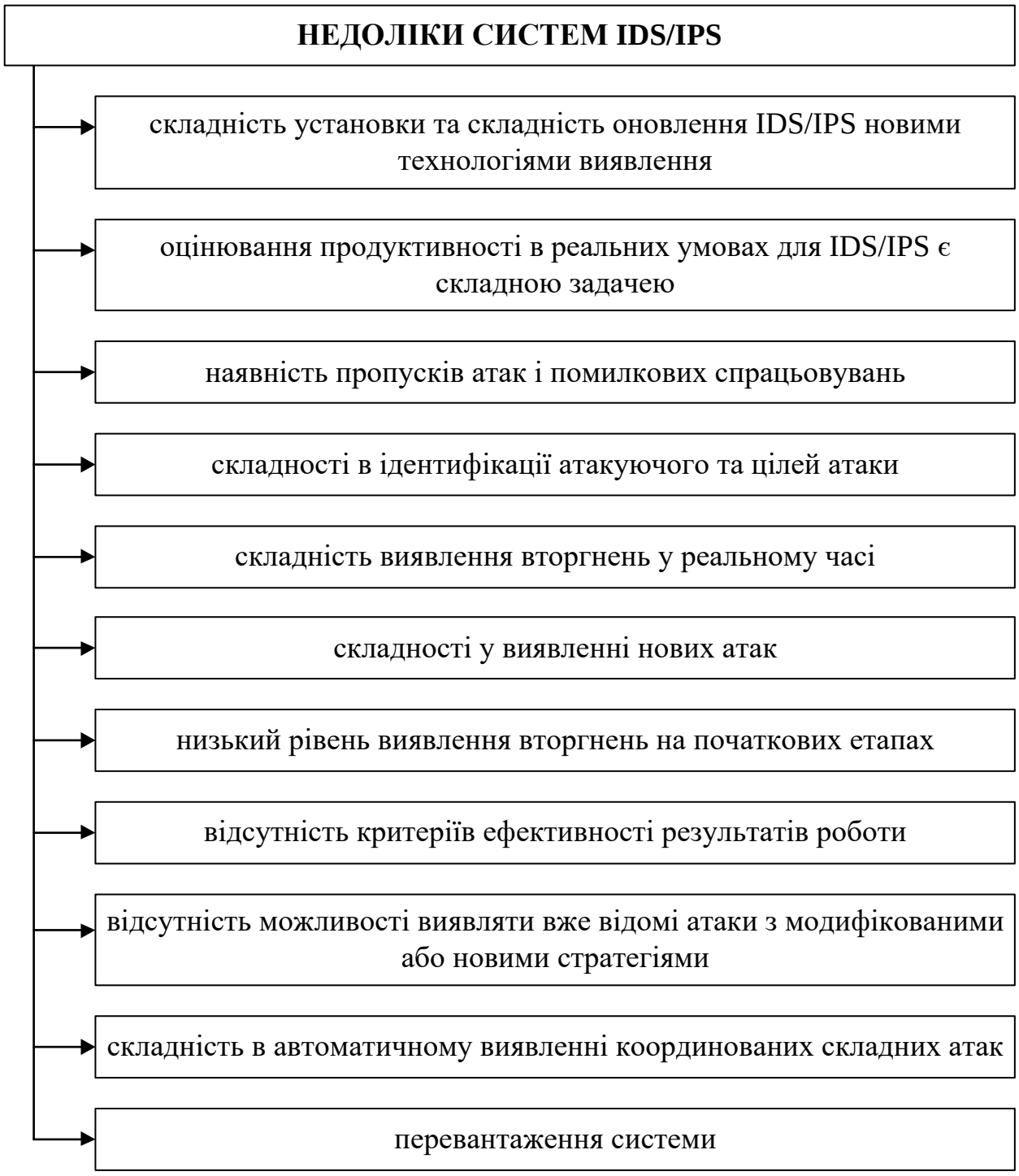

Рисунок 2.9 – Недоліки систем IDS/IPS

Переваги та недоліки основних типів систем виявлення вторгнень [20] наведено в табл. 2.3.

Таблиця 2.3 – Переваги та недоліки різних систем виявлення вторгнень

Тип системи	Переваги	Недоліки
Мережна система виявлення вторгнень (NIDS)	- Повна видимість та контроль мережі. - Аналіз у реальному часі. - Централізоване управління.	- Обмежена перевірка зашифрованого трафіку. - Вплив на продуктивність.
Система виявлення вторгнень на хост (HIDS)	- Поглиблений моніторинг хостів. - Розширений аналіз журналів в режимі реального часу. - Мінімальні витрати на мережу.	- Неповна видимість мережі. - Висока складність керування. - Необхідність регулярних оновлень та обслуговування.
Система виявлення вторгнень на основі сигнатур	- Встановлена та швидка ідентифікація загроз. - Низька частота хибно-позитивних результатів та мінімізація непотрібних тривог та сповіщень.	- Обмежене виявлення загроз нульового дня. - Нездатність виявити поліморфні атаки, що постійно змінюють вигляд.
Система виявлення вторгнень на основі аномалій	- Виявлення невідомих загроз. - Адаптивність до змін у поведінці мережі, пристосування до оновлень, нових програм і шаблонів атак, що розвиваються	- Вищий коефіцієнт хибно-позитивних результатів. - Не ефективне виявлення аномалій в період навчання.

3 ОГЛЯД СУЧАСНИХ РІШЕНЬ IDS/IPS

Сучасний ринок пропонує різноманітні рішення IDS/IPS, кожне з них володіє своїми унікальними функціями та можливостями, призначеними для задоволення потреб різних організацій. На сьогоднішній день найбільшими світовими виробниками систем IDS/IPS є наступні: BAE Systems, Barracuda, Check Point, Cisco, Corero Network Security, Extreme Networks, FireEye, Fortinet, HPE, IBM, Juniper, Kaspersky, McAfee, NSFOCUS, Palo Alto Networks, Radware, SonicWALL, Sophos, Symantec, Trend Micro [21].

Оскільки питання захисту мереж є актуальним, то в інтернеті існує багато публікацій про найкращі системи IDS/IPS, їхні огляди та рейтинги. В різних джерелах рейтинги систем IDS/IPS 2024 року мають різну кількість та різний набір систем, що в нього входять. Аналіз різних джерел [16, 17, 21 – 28] показав, що є системи IDS/IPS, які присутні у всіх рейтингах, а отже є дійсно найкращими та затребуваними. Серед них було обрано 10 найбільш популярних систем (рис. 3.1).

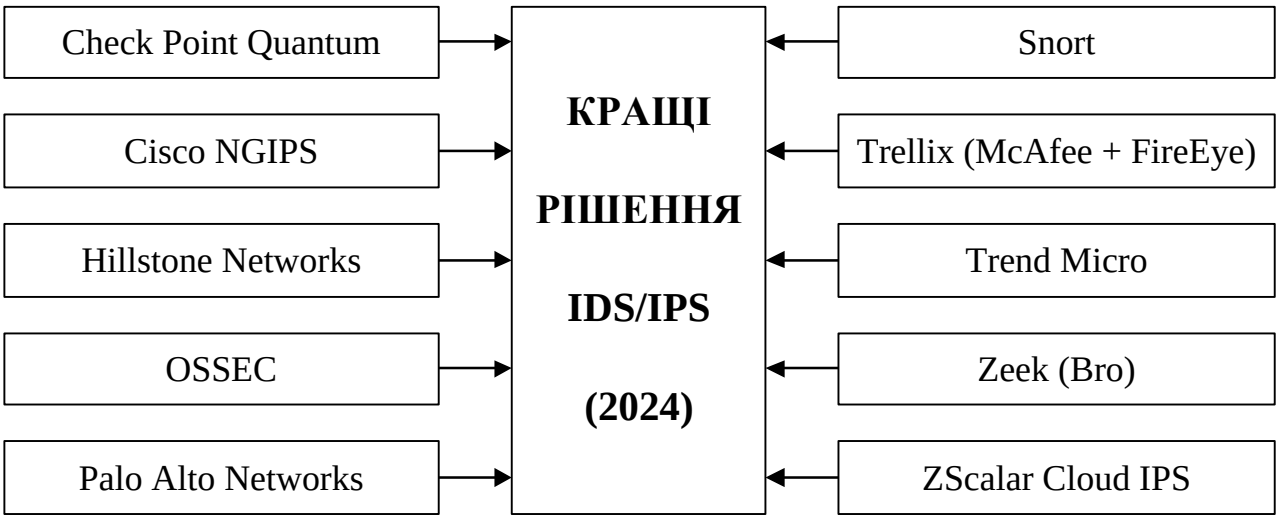

Рисунок 3.1 – Найкращі рішення IDS/IPS

3.1 Check Point Quantum

Check Point [22, 24, 25, 27] вбудовує Quantum IPS у свої рішення брандмауера нового покоління (NGFW) для сканування пакетів, що проходять через пристрій. Цей пристрій може замінити різноманітні інші пристрої (брандмауери, VPN тощо) і забезпечувати функції IDS та IPS [22].

Check Point IDS працює як невід'ємний компонент всебічного пакету безпеки Check Point, наголошуючи на багаторівневому підході до пом'якшення загроз. Цей підхід гарантує, що загрози, незалежно від їх походження чи характеру, вирішуються на різних рівнях, забезпечуючи надійний захист.

Check Point забезпечує інтегровані можливості запобігання вторгненням брандмауера нового покоління на мультигігабітних швидкостях, забезпечуючи високу ефективність безпеки та низький рівень помилкових спрацьовувань. Підхід до глибокого захисту системи поєднує різні методи безпеки, такі як підписи, перевірка протоколів, виявлення аномалій і аналіз поведінки, щоб забезпечити комплексний захист.

3.2 Cisco NGIPS

Cisco [22 – 26] продає свій продукт Secure IPS як систему запобігання вторгненням нового покоління (NGIPS) із понад 35 000 вбудованих правил IPS і широкими можливостями для виявлення та блокування аномального трафіку. Secure IPS можна інтегрувати з іншими пристроями Cisco або розгорнути як окрему IPS [22].

Cisco Secure IPS є частиною системи безпеки Cisco, яка використовує такі методи, як системи виявлення на основі сигнатур, виявлення аномалій і аналіз поведінки для виявлення та пом'якшення загроз. Система запобігання вторгненням може бути реалізована в різних мережних налаштуваннях, таких як фізичні, хмарні або віртуальні пристрої. Система здатна розшифровувати та ретельно перевіряти зашифрований трафік, щоб виявити приховані загрози.

Cisco IDS, засноване на надійних рішеннях безпеки, спеціалізується на захисті розгалужених корпоративних мереж. Його здатність безкомпромісно обробляти великі обсяги трафіку робить його оптимальним вибором для великомасштабних операцій.

3.3 Hillstone Networks

Hillstone Networks [22, 25, 26] пропонує високошвидкісні спеціалізовані пристрої для мережних IPS і брандмауерів нового покоління. Обладнання Hillstone IPS широко використовується та пропонує низку приладів для вирішення різноманітних задач захисту.

Рішення Hillstone Networks – це NIPS, що працює в режимі онлайн на швидкості з'єднання, виконуючи глибоку перевірку пакетів і перевірку складання для всього мережного трафіку. Застосовуючи правила, засновані на різних методологіях (таких як аналіз аномалій протоколу та аналіз сигнатур), він ефективно блокує загрози.

Основні функції цього рішення включають запобігання вторгненням, розширене виявлення загроз, виявлення аномальної поведінки, хмарне програмне середовище, антивірус, фільтрацію URL-адрес і контроль програм, які разом створюють комплексне рішення кібербезпеки. Hillstone також забезпечує надійну функцію звітності з детальною видимістю в різних переглядах, обслуговуючи різних користувачів, таких як адміністратори бізнес-систем, адміністратори безпеки та керівники.

3.4 OSSEC

Рішення OSSEC [22 – 24, 27, 28] – це продукт IDS/IPS для команд будь-якого розміру, що відрізняється набором функцій і прозорою командою продажів. OSSEC пропонує безкоштовний HIDS з відкритим вихідним кодом, який є хорошим вибором для малого та середнього бізнесу.

OSSEC (Open Source Security) виконує аналіз журналів, перевірку цілісності файлів, моніторинг, виявлення руткітів, сповіщення в реальному часі та активне реагування. Це комплексний інструмент безпеки, який допомагає організаціям захистити свою критично важливу інфраструктуру та конфіденційні дані шляхом моніторингу та аналізу активності в їхніх системах.

OSSEC забезпечує детальний аналіз журналів із механізмами попередження про потенційні порушення безпеки. Його функція активного реагування автоматизує реакцію на конкретні загрози, оптимізуючи робочі процеси безпеки. OSSEC може похвалитися можливостями інтеграції з популярними інструментами SIEM і платформами візуалізації, забезпечуючи узгоджене представлення даних і практичну інформацію.

3.5 Palo Alto Networks

Рішення Palo Alto Networks відоме у галузі кібербезпеки [21, 22, 26, 28]. Palo Alto Networks пропонує IPS для великих компаній, яким потрібна підтримка, яка постачається з комерційним рішенням. Їхня мережна IPS може бути розгорнута як апаратне забезпечення, програмне забезпечення (віртуальні машини або контейнери), як хмарний сервіс або інтегрована в брандмауери нового покоління.

Palo Alto Networks використовує передові технології, такі як машинне навчання та автоматизація, щоб полегшити безпечне використання програм у мережних середовищах. Їхні системи запобігання вторгненням користуються перевагами уніфікованої архітектури обробки брандмауерів наступного покоління, що дозволяє проактивно й автоматично перехоплювати кіберзагрози на різних етапах розвитку атаки.

IPS аналізує мережний трафік через усі порти, протоколи та навіть зашифровані канали на наявність потенційних загроз. Він використовує ряд стратегій виявлення, включаючи методи на основі сигнатур, аномалій і політик, щоб ефективно розпізнавати та нейтралізувати загрози.

3.6 Snort

Snort – це класична система виявлення вторгнень у мережу (NIDS) і система запобігання вторгненням (IPS) із відкритим кодом [17, 23, 24].

Рішення Snort призначене для моніторингу мережного трафіку в реальному часі, виявлення шкідливих пакетів і виявлення різних типів атак і вторгнень. Snort використовує мову на основі правил для опису шаблонів трафіку та може аналізувати протоколи, корисне навантаження та заголовки IP-пакетів.

Завдяки своїй надійності та відкритому коду Snort забезпечує глибокий захист мережі. Розрахована на тих, хто цінує прозорість і налаштування, рішення Snort з відкритим кодом пропонує користувачам прямий огляд внутрішньої роботи.

Керована правилами мова Snort дозволяє користувачам точно налаштовувати протоколи виявлення, а його можливості аналізу трафіку в реальному часі забезпечують своєчасне уявлення про мережну активність. Окрім основних функцій, Snort добре інтегрується з іншими платформами безпеки та базами даних, підвищуючи зручність використання та масштаб у більших структурах кібербезпеки.

3.7 Trellix (McAfee + FireEye)

Рішення Trellix Network Security [22, 25, 27] об'єднує в собі досягнення двох відомих виробників McAfee та FireEye.

Деталі щодо продукту мережної безпеки Trellix можуть змінитися найближчим часом, оскільки платформа розширеного виявлення та реагування (XDR) компанії створюється на основі платформи мережної безпеки McAfee (NSP) і продуктів безпеки мережі FireEye. Серія злиттів компаній, брендів і технологій відбулася в липні 2021 року, але оригінальні продукти все ще можна знайти на веб-сайтах окремих компаній [22].

Trellix Network Security призначений для виявлення, блокування та реагування на передові, цілеспрямовані та обхідні кібератаки. Він використовує найсучасніше безсигнатурне виявлення для захисту від розширених загроз, включаючи атаки нульового дня, і генерує сповіщення високої точності, коли це необхідно, щоб забезпечити ефективний аналіз і зменшити втому від попереджень. Завдяки доказам у реальному часі та метаданим рівня 7 це рішення спрощує й автоматизує робочі процеси безпеки, полегшуючи розслідування, перевірку сповіщень, стримування кінцевої точки та реагування на інциденти.

Trellix Network Security може ідентифікувати багатопотокові, багатоетапні атаки, атаки нульового дня, поліморфні атаки та атаки програм-вимагачів, які можуть обійти традиційний захист. Використовуючи машинне навчання та штучний інтелект разом із механізмами кореляції, він забезпечує виявлення в реальному часі та ретроспективну ідентифікацію загроз, а також здатність відстежувати та блокувати бічні загрози в мережах.

3.8 Trend Micro

Рішення IPS від Trend Micro [22, 24 – 27] доступне як фізичний або віртуальний пристрій для розгортання в локальних мережах, приватних хмарах або публічних хмарах.

Trend Micro Deep Discovery – це спеціальне рішення, призначене для виявлення, аналізу та реагування на сучасні приховані програми-вимагачі, їх варіанти та цілеспрямовані атаки. Спеціалізація інструменту на виявленні цілеспрямованих і складних загроз виділяє його серед систем безпеки. Його інтеграція з іншими рішеннями Trend Micro забезпечує багаторівневу безпеку та покращену видимість у цифровому середовищі.

Комплексний аналіз загроз і пріоритезація Trend Micro надає компаніям повну видимість мережі для визначення пріоритетів загроз вразливостей. Це досягається шляхом глибокої перевірки мережного трафіку, що дає змогу

виявляти та блокувати загрози, які можуть бути непомічені традиційними рішеннями безпеки. Вбудована функція перевірки SSL додатково зменшує сліпі зони безпеки, створені зашифрованим трафіком. Система TippingPoint від Trend Micro також пропонує гнучкі варіанти розгортання та захист інвестицій, забезпечуючи негайний і постійний захист від загроз за допомогою стандартних рекомендованих налаштувань.

3.9 Zeek (Bro)

Рішення Zeek – це аналізатор мережного трафіку з відкритим кодом [17, 22 – 24, 28]. Zeek (раніше відомий як Bro) є надзвичайно потужною мережною IDS. Вбудована підтримка сценаріїв Zeek дозволяє багато налаштовувань, в тому числі налаштовування автоматичних відповідей на виявлені загрози. Виробник Zeek пропонує готові фізичні або віртуальні пристрої Zeek як Corelight зі зручним графічним інтерфейсом користувача, сценаріями та додатковою підтримкою.

Zeek глибоко досліджує мережний трафік, витягуючи цінні дані, які допомагають зрозуміти та захистити інформаційне середовище. Для тих, хто віддає перевагу комплексному аналізу трафіку, Zeek є природним вибором.

Zeek вирізняється своїм підходом на основі сценаріїв, що дозволяє настроювати аналіз і журналювати мережний трафік. Це забезпечує гнучкість адаптації до різноманітних ландшафтів загроз, що розвиваються. З точки зору інтеграції Zeek доповнює різноманітні системи SIEM і платформи аналізу загроз, підвищуючи свою корисність у складних архітектурах безпеки.

3.10 ZScalar Cloud IPS

Рішення ZScalar Cloud IPS [22, 25, 26] – це хмарна IPS, розроблена для забезпечення постійного захисту від загроз і видимості для користувачів, незалежно від їх місцезнаходження чи типу з’єднання.

Zscaler Cloud IPS працює повністю з хмари, зміщуючи фокус безпеки на дії користувачів і мережний трафік, а не просто на захист сервера. Він надає можливості дешифрування SSL для підвищення видимості безпеки. Будучи хмарною службою, Zscaler IPS пропонує необмежену пропускну здатність і дає змогу перевіряти весь трафік TLS/SSL без шкоди для продуктивності.

Рішення інтегровано з рядом технологій безпеки, включаючи брандмауери, ізольоване програмне середовище, брокери безпеки доступу до хмари (CASB) і інструменти запобігання втраті даних (DLP), для комплексного підходу до безпеки. Крім того, воно надає контекстну інформацію про поведінку користувачів, використання програм і потенційні загрози безпеці, покращуючи свою ефективність у виявленні загроз і реагуванні на них.

4 ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ СИСТЕМ IDS/IPS

4.1 Переваги та недоліки сучасних рішень IDS/IPS

Аналіз переваг та недоліків сучасних рішень IDS/IPS наведено в табл. 4.1.

Таблиця 4.1 – Переваги та недоліки найкращих рішень IDS/IPS

№	Рішення	Переваги	Недоліки
1	Check Point Quantum	- Інтегрована продуктивність IPS до 15 Гбіт/с. - Детальні та настроювані звіти. - Виявлення вразливостей для HTTP, POP, IMAP, SMTP тощо. - Розширене налаштування політик. - Оновлення кожні дві години. - Антивірус, анти-бот і пісочниця. - Блокує DNS-тунелювання, атаки без підписів, відомі CVE. - Використовує сигнатуру та виявлення аномалій.	- Продається лише як обладнання (захищений шлюз). - Немає підтримки сторонніх (хмарних, віддалених) ресурсів, які не перенаправ-ляються через шлюз. - Для захисту внутріш-ній мережний трафік має бути спрямований через шлюз.
2	Cisco NGIPS	- Апаратне та віртуальне розгортання. - Виявлення безфайлових загроз. - Вбудована безпека DNS, IP та URL. - Аналіз загроз та оцінка, пісочниця. - Інтегрує Snort 3.0. - Використовує сигнатуру та виявлення аномалій.	- Не дуже зручний інтерфейс - Вимагає багато пам’яті та потужності. - Ціни залежать від різних параметрів. - Дороге рішення.

Продовження табл. 4.1

№	Рішення	Переваги	Недоліки
3	Hillstone Networks	- 13 000 вбудованих підписів, спеціальні підписи та виявлення аномалій. - Пісочниці для розслідування. - Виявлення від рівня 3 до рівня 7. - Параметри захисту від спаму та блокування URL-адрес. - Хмарне керування розподіленими пристроями.	- Пропозиції лише для приладів. - Техніку потрібно буде оновити, щоб відповідати зростанню. - Дороге рішення.
4	OSSEC	- З відкритим кодом і безкоштовно. - Моніторинг реєстру Windows. - Виявлення ескалації привілеїв MacOS. - Відстежує контрольні суми файлів журналу для виявлення втручання. - Широко використовується – понад 500 000 завантажень на рік.	- Обмежена підтримка Windows. - Крута крива навчання. - Захист зосереджений на системних файлах і не захищає від інших видів атак.
5	Palo Alto Networks	- Постійно оновлювані профілі захисту - Блокує шкідливі сайти, неправильні пакети, повторне збирання TCP, дефрагментацію IP і атаки C2. - Анліз підпису та аномалій. - Розгортання правил Snort і Suricata. - Хмарний нативний варіант. - Інтегрований захист від вразливостей, зловмисного та шпигунського ПЗ. - Сканування зашифрованого трафіку.	- Дорогий варіант. - Відсутність видимості деталей аналізу файлів. - Конфігурації somle мають надто складні етапи впровадження. - Деякі користувачі скаржаться на рівень підтримки.

Продовження табл. 4.1

№	Рішення	Переваги	Недоліки
6	Snort	- З відкритим кодом і безкоштовно. - Встановлюється на Linux, Unix або MacOS, але підтримує аналіз Windows. - Велика бібліотека попередньо створених правил виявлення. - Сніфер, реєстратор пакетів, виявлення вторгнень. - Аналіз сигнатур і аномалій. - Глибоке бачення мережного трафіку - Підтримується Cisco. - Базові правила можна завантажити, платний розширений доступ.	- Нестабільні оновлення. - Залежить від підтримки громади. - Дуже складний із крутою кривою навчання.
7	Trellix (McAfee + FireEye)	- Захист від ботів, DDoS атак, програм-вимагачів та багатьох інших атак. - Блокування шкідливих сайтів та завантажень. - Захищає хмарні та локальні пристрої. - FireEye зосереджена на виявленні аномалій, McAfee – на виявленні сигнатур. - Запуск на фізичних або віртуальних пристроях. - Можливості пісочниці. - Виявлення та блокування зловмисного ПЗ, фішинг, експлойти, командно-контрольні (C2) зворотні виклики та ботнети.	- Хибні спрацьовування для виявлення шкідливих сайтів. - Негативно впливає на продуктивність мережі. - Ціни будуть заплутаними, доки старіші продукти не будуть припинені.

Продовження табл. 4.1

№	Рішення	Переваги	Недоліки
8	Trend Micro	- Включає антивірусні сигнатури Trend Micro, а також машинне навчання. - Можливість пісочниці для дослідження. - Розгортання з правилами та політиками безпеки для блокування поточних і попередніх загроз. - Використовує глибоку перевірку пакетів, аналіз шкідливих програм, репутацію URL-адреси та репутацію загрози. - Застосовує сигнатурний аналіз і аналіз аномалій. - Сканує вхідний, вихідний і бічний трафік.	- Ще не інтегрується з іншими продуктами IPS або TrendMicro (DBI, IWSVA тощо). - Автоматичне застосування правил може порушити бізнес-процеси. - Дорогий варіант.
9	Zeek (Bro)	- З відкритим кодом доступний безкоштовно. - Працює в системах MacOS і *nix. - Глибоке бачення мережного трафіку - Інтегрована реєстрація трафіку. - Завдання дозволяють налаштувати автоматизацію. - Відстежує трафік SNMP і активність FTP, DNS і HTTP. - Виконує аналіз на прикладному рівні для ширшого аналізу. - Застосовує як сигнатуру, так і виявлення аномалій.	- Крута крива навчання, вимагає глибоких знань SIEM та IDS. - Безкоштовна версія з відкритим кодом не підтримується. - Недоступно для Windows.

Продовження табл. 4.1

№	Рішення	Переваги	Недоліки
10	ZScalar Cloud IPS	- Підтримує всі типи ресурсів: локальні дані, хмарні дані, програми SaaS. - Масштабоване вимірюване рішення, яке збільшується або зменшується за потреби. - Може розшифрувати трафік SSL. - Необмежена ємність. - Не потрібно купувати апаратне забезпечення чи керувати програмним забезпеченням. - Команди безпеки можуть досліджувати сповіщення IPS і отримати доступ до бібліотеки загроз для отримання додаткової інформації. - Підтримує iOS, macOS, Android, Windows, деякі Linux. - Підтримує мобільні пристрої.	- Пропонується лише як ліцензія SaaS. - Може підтримувати не всі ОС. - Може додати затримку продуктивності мережі. - Глобальна інсталяція та користувальницьке вирівнювання програми можуть бути складними та трудомісткими.

Різні сучасні рішення мають свої особливості, можливості, свій спектр дії. Тому при виборі оптимального рішення перш за все необхідно проаналізувати переваги та недоліки кожного з них.

4.2 Порівняння та вибір найкращих рішень IDS/IPS

Не кожна система виявлення та запобігання вторгненням однакова. Рішення IDS/IPS використовують різні методи виявлення, місце дії, різні об'єкти захисту, саме тому для вибору рішення для впровадження в конкретній

ситуації важливо розуміти мету, вимоги та особливості даної інформаційної мережі.

Виходячи з конкретних потреб і унікальних проблем, пов’язаних із безпекою мережі, необхідно визначити які саме параметри та їхні характеристики необхідно врахувати при виборі рішення IDS/IPS. Основні параметри (рис. 4.1), що пов’язані з точністю виявлення, масштабованістю та інтерфейсом можуть характеризувати якість рішення IDS/IPS.

Рисунок 4.1 – Показники якості рішення IDS/IPS

Основна функціональність рішення IDS/IPS визначається точною ідентифікацію відомих і невідомих загроз в режимі реального часу, можливістю запобігання виявленим загрозам, аналізом мережного трафіку на наявність ненормальних шаблонів, які можуть вказувати на потенційну загрозу, а також

наявністю сповіщень в реальному часі про загрози та комплексних звітів для аналізу.

Ключові особливості рішення IDS/IPS визначаються можливостями інструменту розвиватися з появою загроз і розпізнавати шаблони в даних, злагодженою роботою системи з іншими рішеннями безпеки в екосистемі організації, налаштуваннями чутлиості на основі мережного середовища для мінімізації помилкових спрацьовувань, аналізом зашифрованіих пакетів даних без шкоди для безпеки, оновленнями інформації про нові загрози.

Важливими також є параметри юзабіліті. Головна консоль має надавати чіткий огляд стану безпеки мережі, включаючи виявлені загрози, моделі трафіку та стан системи. Замість складного кодування зручний інтерфейс для налаштування правил допомагає швидше налаштовувати та розгортати. Контроль доступу на основі ролей важливий для великих команд, це дозволяє встановлювати спеціальні дозволи для різних користувачів, гарантуючи, що лише авторизований персонал може вносити зміни або отримувати доступ до конфіденційної інформації. Враховуючи складність деяких інструментів, наявність доступних навчальних ресурсів, документації та оперативної підтримки клієнтів є теж дуже важливими.

Порівняння рішень IDS/IPS наведено в табл. 4.2.

Таблиця 4.2 – Порівняння рішень IDS/IPS

Рішення	IDS, IPS та місце дії	Підтримувані платформи	Виявлення	Вартість
Check Point Quantum	IDS, IPS, мережа	Пристрій	Широке виявлення загроз	$1500+ на рік
Cisco NGIPS	IPS, мережа	Пристрій, віртуальна машина	Широке виявлення загроз	$1280+ на рік

Продовження табл. 4.2

Рішення	IDS, IPS та місце дії	Підтримувані платформи	Виявлення	Вартість [22]
Hillstone Networks	IDS, IPS, мережа	Пристрій	Широке виявлення загроз	Безстрокова ліцензія на основі користу-вачів і функцій
OSSEC	IDS, IPS, хост	Unix, Linux, MacOS, Windows	Моніторинг системних файлів	Безкоштовно
Palo Alto Networks	IDS, IPS, мережа	Пристрій, віртуальна машина	Широке виявлення загроз	$9509,50+
Snort	IDS, IPS, мережа	Linux, Unix, MacOS	Широке виявлення загроз	Безкоштовно, $399+ за підпис-ку на правила
Trellix (McAfee + FireEye)	IDS, IPS, мережа	Пристрій або програмне забезпечення	Широке виявлення загроз	$10 995+
Trend Micro	IDS, IPS, мережа	Пристрій або програмне забезпечення	Широке виявлення загроз	Інформація недоступна
Zeek (Bro)	IDS, мережа	Windows, Linux, Unix, MacOS	Широке виявлення загроз	Безкоштовно
ZScalar Cloud IPS	IDS, IPS, мережа, хмара	Windows, MacOS, трохи Linux, Android, iOS	Широке виявлення загроз	Пропонує різні рівні: бізнес, трансформація тощо

З табл.. 4.3 можна зробити наступні висновки: оскільки для порівняння було обрано найкращі 10 актуальних систем IDS/IPS, то всі вони мають чудові показники виявлення та запобігання вторгнень. Відрізняються вони платформами, що використовують, ціною та місцем розгортання. Однозначно визнати будь-яку з цих систем переважнішою за інші не можна. Але якщо враховувати вимоги та конкретну ситуацію для впровадження рішення IDS/IPS, то можна сформувати деякі рекомендації (табл.. 4.3).

Таблиця 4.3 – Вибір рішення IDS/IPS для конкретних ситуацій

№	Рішення	Ситуація
1	Check Point Quantum	найкраще рішення для багаторівневих стратегій безпеки
2	Cisco NGIPS	найкраще рішення для великих підприємств
3	Hillstone Networks	найкраще рішення для багаторівневого запобігання загрозам
4	OSSEC	найкраще рішення для керування та аналізу журналів
5	Palo Alto Networks	найкраще рішення для автоматичної нейтралізації загроз на різних етапах розвитку атак
6	Snort	найкраще рішення з відкритим кодом для малих та середніх компаній
7	Trellix (McAfee + FireEye)	найкраще рішення для компаній, які можуть виділити значний бюджет на захист своєї мережі, для інтегрованого та розширеного аналізу загроз
8	Trend Micro	найкраще рішення для цілеспрямованої ідентифікації атак
9	Zeek (Bro)	найкраще для аналізу мережного трафіку
10	ZScalar Cloud IPS	найкраще для постійного захисту від загроз і видимості для користувачів, незалежно від їх місцезнаходження чи типу з’єднання і без шкоди для продуктивності.

Організації можуть вибирати з низки недорогих і потужних рішень IDS і IPS, які відповідають різноманітним потребам - від стартапів з обмеженим бюджетом до глобальних підприємств. Деякі з них будуть окремими рішеннями, а інші – функціями, доданими до інших продуктів безпеки.

Таким чином, для вибору найкращої системи виявлення та запобігання вторгнень необхідно проаналізувати всі особливості та потреби компанії для захисту мережі, а також оцінити можливості, особливості, вартість, переваги та недоліки рішень IDS/IPS, для того щоб обрати найбільш відповідне рішення для впровадження в інформаційні мережі компанії.

Варто зазначити, що рішення IDS/IPS не є універсальним підходом до безпеки мережі. Його найкраще впроваджувати разом із кількома іншими заходами кібербезпеки для посилення захисту. Сьогодні системи IDS/IPS все частіше розглядають як частину більш повного комплексного рішення безпеки.

ВИСНОВКИ

Сучасні інформаційні мережі є складними та перевантаженими, вони мають багато точок доступу та мають справу з великим обсягом трафіку, що робить вкрай необхідним вчасний та ефективний моніторинг і реагування. Крім того, загрози, з якими стикаються корпоративні системи безпеки, стають дедалі численнішими та складнішими. Автоматизовані можливості IDS/IPS є життєво важливими в цій ситуації, оскільки дозволяють компаніям швидко реагувати на загрози, не створюючи при цьому навантаження на IT-команди. Будучи частиною інфраструктури безпеки компанії, IDS/IPS є важливим засобом запобігання серйозних і складних атак.

В роботі було розглянуто та проаналізовано ряд питань, що стосуються сучасних систем виявлення та запобігання вторгнень.

В першому розділі проаналізовано проблеми безпеки в інформаційних мережах, розглянуто інструменти мережної безпеки, засоби виявлення та усунення вразливостей , засоби виявлення та запобігання вторгнень.

В другому розділі досліджено функціонал систем IDS/IPS, архітектуру та принцип роботи IDS/IPS. Наведено класифікацію систем IDS/IPS. Розлянуто переваги та недоліки IDS/IPS.

Третій розділ присвячено огляду сучасних рішень IDS/IPS, а саме Check Point Quantum, Cisco NGIPS, Hillstone Networks, OSSEC, Palo Alto Networks, Snort, Trellix (McAfee + FireEye), Trend Micro, Zeek (Bro) та ZScalar Cloud IPS.

В четвертому розділі виконано порівняльний аналіз найбільш популярних сучасних рішень IDS/IPS, розглянутих в третьому розділі. Проаналізовано переваги та недоліки цих рішень. Проведено порівняння сучасних рішень IDS/IPS за основними характеристиками та виконано вибір кращих ріщень для різних ситуацій.

Сучасний ринок пропонує багато різноманітних рішень для виявлення та запобігання вторгненням, починаючи від відкритих і закінчуючи комерційними

варіантами. Усі розглянуті системи IDS/IPS мають свої особливості та переваги. Тому вибір найкращої системи буде змінюватись в залежності від обставин, умов та потреб конкретної мережі.

Вибір того, що використовувати, має ґрунтуватися на унікальних потребах і ресурсах організації. Бюджет, персонал, IT-середовище, стійкість до ризику та бізнес-стратегії відіграють важливу роль у визначенні того, яке рішення забезпечить хорошу відповідність.

Впроваджуючи надійні методи безпеки, навчаючи співробітників і регулярно переглядаючи й оновлюючи заходи безпеки, можна створити стійкий захист від загроз, що постійно розвиваються в цифровому світі.

Результати роботи було апробовано на XXVIII Міжнародному молодіжному форумі «Радіоелетроніка і молодь у XXI столітті» в рамках конференції «Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій» та опубліковано тези доповіді [29] за тематикою кваліфікаційної роботи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Закон України Про електронні комунікації [Електронний ресурс] // Верховна Рада України. Законодавство України. – 2024. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

2. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: навч. посібник / Г. М. Гулак. – Київ: Видавництво НА СБ України, 2020. – 256 с.

3. Phipps J. Top 19 Network Security Threats + Defenses for Each [Електронний ресурс] / Jenna Phipps // eSecurity Planet. – 2024. – Режим доступу до ресурсу: https://www.esecurityplanet.com/networks/network-security-threats/.

4. What is a Network Attack? Network attacks and network security threats explained [Електронний ресурс] // Forcepoint. – 2024. – Режим доступу до ресурсу: https://www.forcepoint.com/cyber-edu/network-attack.

5. Spasojevic A. Network Security Threats Explained [Електронний ресурс] / Anastazija Spasojevic // Phoenix NAP. – 2023. – Режим доступу до ресурсу: https://phoenixnap.com/blog/network-security-threats.

6. Verma A. Common network security vulnerabilities [Електронний ресурс] / Apporwa Verma // Cobalt. – 2023. – Режим доступу до ресурсу: https://www.cobalt.io/blog/common-network-security-vulnerabilities.

7. Moore M. Top Cybersecurity Threats in 2023 [Електронний ресурс] / Michelle Moore // University of San Diego. – 2023. – Режим доступу до ресурсу: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/.

8. All What you Need to Know about Network Security Tools [Електронний ресурс] // CyberTalents. – 2024. – Режим доступу до ресурсу: https://cybertalents.com/blog/network-security-tools.

9. What Are Network Security Tools [Електронний ресурс] // LeoNetworkGroup. – 2023. – Режим доступу до ресурсу: https://www.leonetworkgroup.com/news/what-are-network-security-tools.html.

10. Vulnerability Management – From Detection to Mitigation [Електронний ресурс] // Truesec. – 2024. – Режим доступу до ресурсу: https://www.truesec.com/security/vulnerability-management-from-detection-to-mitigation.

11. Penetration Testing: Methodology, Scope and Types of Pentests [Електронний ресурс] // Vaadata. – 2024. – Режим доступу до ресурсу: https://www.vaadata.com/blog/penetration-testing-methodology-scope-and-types-of-pentests/.

12. Firewalls, Intrusion Prevention and VPNs [Електронний ресурс] // University of Houston-Clear Lake. – 2024. – Режим доступу до ресурсу: https://www.uhcl.edu/information-security/tips-best-practices/firewalls.

13. Mohanakrishnan R. What Is Intrusion Detection and Prevention System? Definition, Examples, Techniques, and Best Practices [Електронний ресурс] / Ramya Mohanakrishnan // Spiceworks. – 2022. – Режим доступу до ресурсу: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-idps/#lg=1&slide=0.

14. Bhardwaj R. Difference between IPS and IDS – Download Detailed Comparison Table [Електронний ресурс] / Rashmi Bhardwaj // Ipwithease. – 2024. – Режим доступу до ресурсу: https://ipwithease.com/difference-between-ips-and-ids-in-network-security/.

15. Swanagan M. Intrusion Detection VS Prevention Systems: What's The Difference? [Електронний ресурс] / Michael Swanagan // Purplesec. – 2023. – Режим доступу до ресурсу: https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/.

16. Thapa S. The role of intrusion detection/prevention systems in modern computer networks: a review [Електронний ресурс] / S. Thapa, A. Dissanayaka // Midwest Instruction and Computing Symposium (MICS2020). – 2020. – Режим доступу до ресурсу: https://www.micsymposium.org/mics_2020_Proceedings/MICS2020_paper_1.pdf.

17. Коробейнікова Т. І. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень / Т. І. Коробейнікова, О. О. Цар. // Міжнародний науковий журнал «Грааль науки». – 2023. – № 27. – С. 317 – 325.

18. Intrusion Detection & Prevention Systems Guide [Електронний ресурс] / // Trend Micro. – 2023. – Режим доступу до ресурсу: https://www.trendmicro.com/en_us/ciso/22/l/intrusion-detection-prevention-systems.html.

19. Лукова-Чуйко В. Н. Методи виявлення вторгнень у сучасних системах IDS / В. Н. Лукова-Чуйко, С. В. Толюпа, І. І. Пархоменко. // Безпека інформаційних систем і технологій. – 2021. – № 1 (5). – С. 19 – 26.

20. Advantages and disadvantages of intrusion detection system (IDS) types [Електронний ресурс] // General International Group. – 2024. – Режим доступу до ресурсу: https://generalintlgroup.com/en/blog/advantages-and-disadvantages-of-intrusion-detection-system-ids-types.

21. Intrusion Detection Systems / Intrusion Prevention Systems (IDS/IPS) Market - Insights and Trends | 2031 [Електронний ресурс] // Linked in. – 2024. – Режим доступу до ресурсу: https://linkedin.com/pulse/intrusion-detection-systems-prevention-1mgif.

22. Samson R. Top 10 Intrusion Detection And Prevention Systems [Електронний ресурс] / Ron Samson // Clearnetwork. – 2023. – Режим доступу до ресурсу: https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/.

23. Trisolino A. Analysis of Security Configuration for IDS/IPS : Master of Science in Computer Engineering / Trisolino Andrea – Politecnico di Torino, 2023. – 92 p.

24. Miguel P. G. 26 Best Intrusion Detection Software in 2024 Unveiled [Електронний ресурс] / Paulo Gardini Miguel // The CTO. – 2024. – Режим доступу до ресурсу: https://thectoclub.com/tools/best-intrusion-detection-software/.

25. McDade M. The Top 10 Intrusion Prevention System Solutions [Електронний ресурс] / Mirren McDade // Expert Insights. – 2024. – Режим

доступу до ресурсу: https://expertinsights.com/insights/top-intrusion-prevention-systems/.

26. Karatas G. Top 12 Intrusion Detection and Prevention Tools in 2024 [Електронний ресурс] / Gulbahar Karatas // AIMultiple. – 2024. – Режим доступу до ресурсу: https://research.aimultiple.com/ips-tools/.

27. Phipps J. 6 Best Intrusion Detection & Prevention Systems for 2024 [Електронний ресурс] / Jenna Phipps // eSecurity Planet. – 2024. – Режим доступу до ресурсу: https://www.esecurityplanet.com/products/intrusion-detection-and-prevention-systems/.

28. Top 10 Best Intrusion Detection Systems (IDS) [2024 Rankings] [Електронний ресурс] // Software Testing Help. – 2024. – Режим доступу до ресурсу: https://www.softwaretestinghelp.com/intrusion-detection-systems/.

29. Михайлова А.С., Чеботарьова Д.В. Аналіз систем виявлення та запобігання вторгнень для захисту інформаційних мереж / Науковий керівник – к.т.н., доц. Чеботарьова Д.В. // Тези доповідей 28-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». Збірник матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2024. – С. 140 – 141.