

Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“___” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за першим (бакалаврським) рівнем вищої освіти
на тему
“Програмне забезпечення системи кібербезпеки для
спостереження за мережевою активністю з використанням Deep
Packet Inspection”

Виконав здобувач вищої освіти
IV курсу, групи КБ-22-2
ОПП «Кібербезпека»
спеціальності 125 «Кібербезпека»
_____ Красніцька Є.А.
«___» _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Смірнова Т.В.
«___» _____ 2026 р.
Рецензент _____

Центральноукраїнський національний технічний університет
Факультет Механіко-технологічний
Кафедра Кібербезпеки та програмного забезпечення
Освітній ступінь бакалавр
Галузь знань 12 "Інформаційні технології"
Спеціальність 125 "Кібербезпека"
Освітньо-професійна (освітньо-наукова) програма "Кібербезпека"

ЗАТВЕРДЖУЮ

Завідувач кафедри

д.т.н., проф.

_____ Олексій СМІРНОВ

« 27 » лютого 2026 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ПЕРШИМ (БАКАЛАВРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Красніцькій Єлизаветі Андріївні

(прізвище, ім'я, по батькові)

1. Тема роботи *Програмне забезпечення системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection*

2. Керівник роботи *Смірнова Тетяна Віталіївна, канд. техн. наук, доцент*

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 129-02 від 27.02.2026 року

3. Строк подання студентом роботи до захисту 23.05.2026 р.

4. Мета та завдання випускної кваліфікаційної роботи: *Метою роботи є розробка програмного забезпечення системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection*

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Призначення та область використання.

2. Перегляд аналогічних існуючих систем.

3. Опис і обґрунтування проектних рішень.

4. Етапи програмування системи.

5. Впровадження системи кібербезпеки в промислову експлуатацію.

6. Висновки

6. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Структурна схема системи кібербезпеки 1 аркуш

Функціональна схема системи кібербезпеки 1 аркуш

Діаграма процесів 1 аркуш

Блок-схема алгоритму роботи додатку 2 аркуша

7. Дата видачі завдання « 27 » лютого 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.03.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.03.2026 р.	
3.	Розробка моделі компонента	20.03.2026 р.	
4.	Розробка структур даних	25.03.2026 р.	
5.	Розробка алгоритмів зв'язку та відображення	30.03.2026 р.	
6.	Програмування алгоритмів	10.04.2026 р.	
7.	Оформлення ПЗ	17.04.2026 р.	
8.	Попередній захист роботи	23.05.2026 р.	

Дата видачі завдання
« 27 » лютого 2026 р.

Підпис керівника

Смірнова Т.В.
(прізвище та ініціали)

Завдання прийнято до виконання
« 27 » лютого 2026 р.

Підпис здобувача

Красніцька Є.А.
(прізвище та ініціали)

АНОТАЦІЯ

Красніцька Є.А. Програмне забезпечення системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection. 125 Кібербезпека. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection.

Метою розробки є програмне забезпечення системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection.

Результат роботи – програмна реалізація системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі Python.

Ключові слова: кібербезпека, Deep Packet Inspection

ABSTRACT

Krasnitska E.A. Software for a cybersecurity system for monitoring network activity using Deep Packet Inspection. 125 Cybersecurity. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification work for the first (bachelor's) level of higher education, software has been developed that is intended for a cybersecurity system for monitoring network activity using Deep Packet Inspection.

The purpose of the development is to develop software for a cybersecurity system for monitoring network activity using Deep Packet Inspection.

The result of the work is a software implementation of a cybersecurity system for monitoring network activity using Deep Packet Inspection.

In the process of working on the software model, an analysis of existing hardware and software was performed. All components of the developed software are fully described.

A convenient user interface has been developed. Instructions for working with software are provided.

The program can be used on PCs with Windows 10/11.

The program is developed in the Python environment.

Keywords: cybersecurity, Deep Packet Inspection

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ	2
ВСТУП.....	3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ	5
1.1 Призначення системи.....	5
1.2 Область застосування.....	5
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ	7
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти.....	7
2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування.....	13
2.3 Розгорнута постановка завдання	15
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	17
3.1 Опис функціонування системи	17
3.2 Розробка структурної схеми.....	32
3.3 Розробка функціональної схеми	39
3.4 Розробка діаграми процесів.....	52
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	54
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	54
4.2 Захист розробленого програмного забезпечення.....	70
5 ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	71
6 ОСНОВНІ ВИСНОВКИ.....	78
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	80

					ВКРБ-125.26.0035.00.00.ПЗ			
Вим.	Арк.	№ докум.	Підп.	Дата	<i>Програмне забезпечення системи кібербезпеки для спостереження за мережевою активністю з використанням Deer Packet Inspector</i>	Літ.	Аркуш	Аркушів
<i>Розроб.</i>	Красніцька Є.А.					Б	1	86
<i>Перев.</i>	Смірнова Т.В.							
<i>Н.контр.</i>	Коваленко А.С.					ЦНТУ КБ-22-2		
<i>Затв.</i>	Смірнов О.А.							

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЛОМ	—	локальна обчислювальна мережа
MME	—	міжмережні екрани
ATM	—	асинхронний режим передачі
BSD	—	адаптована для Internet реалізація операційної системи UNIX
ICMP	—	міжмережний протокол управляючих повідомлень
IP	—	Internet Protocol – міжмережний протокол
NFS	—	мережна файлова система
PPP	—	протокол передачі від точки до точки
RFC	—	опис набору протоколів Internet
RPC	—	віддалений виклик процедури
SLIP	—	міжмережний протокол для послідовного каналу
SMTP	—	Simple Mail Transfer Protocol – простий протокол передачі пошти
TCP	—	Transmission Control Protocol – протокол управління передачею
UDP	—	User Datagram Protocol – протокол користувальницьких датаграм
UNIX	—	багатозадачна операційна система
UTP	—	незахищена вита пара
URL	—	уніфікований покажчик інформаційного ресурсу

ВСТУП

Актуальність теми. Глобальний ринок глибокої перевірки пакетів (Deep Packet Inspection) оцінювався в 33,65 мільярда доларів США у 2025 році та, за прогнозами, зросте з 42,13 мільярда доларів США у 2026 році до приблизно 298,70 мільярда доларів США до 2035 року, зростаючи зі середньорічним темпом зростання (CAGR) 24,40% з 2026 по 2035 рік. Зростання ринку глибокої перевірки пакетів зумовлене зростаючою стурбованістю щодо безпеки мережі та оптимізації продуктивності.

Ключові висновки ринку глибокої перевірки пакетів:

- Північна Америка домінувала на ринку з найбільшою часткою ринку в 39% у 2025 році.
- Очікується, що Європа зазнає найшвидшого зростання в найближчі роки.
- За компонентами, сегмент рішень займав найбільшу частку ринку – 74% у 2025 році.
- За компонентами, за прогнозами, сегмент послуг зростатиме з найшвидшим середньорічним темпом зростання (CAGR) на рівні 27% протягом прогнозованого періоду.
- За розгортанням, локальний сегмент займав найбільшу частку ринку у 2025 році.
- Очікується, що після розгортання хмарний сегмент зростатиме з найвищим середньорічним темпом зростання (CAGR) протягом оціночного періоду.
- За кількістю встановлених пристроїв, інтегрований сегмент домінував на ринку глибокої перевірки пакетів у 2025 році.
- Завдяки встановленню, сегмент автономних систем, ймовірно, зростатиме з найвищими середньорічними темпами зростання (CAGR) у найближчі роки.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

- За розміром підприємств, сегмент великих підприємств домінував на ринку у 2025 році.
- За розміром підприємств очікується, що сегмент малих та середніх підприємств (МСП) швидко зростатиме в найближчому майбутньому.
- За застосуванням, сегмент мережевої безпеки домінував на ринку з найбільшою часткою у 2025 році.
- За кінцевим використанням, сегмент банківської справи, фінансових послуг та страхування (BFSI) лідирував на ринку у 2025 році.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем для спостереження за мережевою активністю з використанням Deep Packet Inspection.
- Дослідження системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection.
- Програмна реалізація системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі для спостереження за мережевою активністю з використанням Deep Packet Inspection.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Ринок глибокої перевірки пакетів демонструє швидке зростання завдяки зростаючій увазі до оптимізації продуктивності мережі. DPI – це технологія, яка дозволяє мережевим операторам аналізувати трафік у режимі реального часу та диференціювати його відповідно до корисного навантаження. Вона знаходить застосування в мережевій безпеці та управлінні трафіком, покращуючи продуктивність мережі. Приватні та державні організації використовують DPI для перевірки вмісту пакетів даних. Вона стала ключовим інструментом для урядових організацій для виявлення загроз та кібератак, які не видно у вмісті пакетів даних. Зростаюча потреба в мережевій безпеці ще більше стимулює зростання ринку.

Інтеграція штучного інтелекту в глибоку перевірку пакетів (DPI) підвищує точність виявлення загроз, тим самим покращуючи безпеку мережі. ШІ може аналізувати величезні обсяги мережових даних для виявлення аномалій у мережі. Це значно покращує можливості фільтрації мережі та виявлення трафіку. DPI на базі ШІ може додатково оптимізувати продуктивність мережі, аналізуючи шаблони трафіку та зменшуючи затримку. Рішення DPI на базі ШІ ефективно запобігають шахрайській діяльності та виявляють її, вирішуючи проблеми безпеки.

1.2 Область застосування

Фактори зростання ринку глибокої перевірки пакетів:

– Зростаючий попит на рішення для управління трафіком даних стимулює зростання ринку глибокої перевірки пакетів. DPI надає детальну аналітику

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

моделей використання мережі, дозволяючи операторам розставляти пріоритети та ефективніше використовувати пропускну здатність. Це забезпечує безперебійний користувацький досвід на тлі зростання коефіцієнтів використання даних.

– Досягнення в технологіях, таких як Інтернет речей (IoT) та мережеві пристрої 5G, ще більше стимулюють зростання ринку. Зі збільшенням розвитку та впровадження технологій 5G також зростає потреба в ефективних рішеннях для оптимізації продуктивності та безпеки мережі.

– Зростаюча кількість кібератак сприяє розширенню ринку.

Перспективи ринку:

– Огляд зростання галузі: Ринок глибокої перевірки пакетів переживає бум через кіберзагрози, стрімке зростання інтернет-трафіку та необхідність дотримання нормативних вимог.

– Глобальна експансія: Північна Америка прогресує найшвидше, за нею йде Європа, а Азіатсько-Тихоокеанський регіон швидко нарощує темпи завдяки впровадженню ініціатив цифрової трансформації.

– Основні інвестори: Cisco Systems, Palo Alto Networks, Juniper Networks, Sandvine та Huawei – це основні інвестори, які сприяють інноваціям на ринку.

– Екосистема стартапів: Стартапи звертають увагу на хмарні та штучно-керовані продукти DPI, що вирішують проблеми складності зашифрованого трафіку та витонченого виявлення загроз.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти

Керування сучасною корпоративною мережею схоже на управління повітряним рухом для тисяч одночасних, невидимих польотів. Якщо ви перевіряєте лише, чи злетів і приземлився літак, ви пропускаєте турбулентність, об'їзди в повітрі та неавторизованих пасажирів. Оскільки складність мережі швидко зростає через гібридні хмарні системи, віддалену робочу силу та сильно зашифрований трафік у 2026 році, покладатися на поверхневі інформаційні панелі більше не є життєздатним. Глибока видимість мережі стала важливою як для виявлення загроз, так і для оптимізації продуктивності.

Для IT-директорів та IT-лідерів пріоритети різко зміщуються навколо безпеки та відповідності. Зі збільшенням трафіку глобальної корпоративної мережі та зростанням розподілених архітектур, прогалини у видимості – це те, де процвітають кіберзлочинці та починаються перебої, що виснажують доходи. Видимість на рівні пакетів забезпечує незаперечну «правду» про те, що рухається вашими цифровими каналами, дозволяючи командам SRE та SOC точно визначити першопричину проблем з продуктивністю та нейтралізувати загрози безпеці, перш ніж вони посиляться.

Програмне забезпечення для перехоплення пакетів слугує мікроскопічною лінзою для вашого мережевого трафіку. Коли дані передаються через Інтернет або локальну інтрамережу, вони розбиваються на невеликі, керовані одиниці, які називаються «пакетами». Перехоплення пакетів (або аналіз мережевих пакетів) – це процес перехоплення, реєстрації та перевірки цих окремих пакетів під час їх проходження через вашу інфраструктуру. У ширшому контексті кібербезпеки та

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7

мережевого моніторингу це програмне забезпечення діє як високотехнологічний засіб прослуховування. У той час як стандартні інструменти моніторингу можуть повідомляти вам про перевантаження пропускної здатності сервера, програмне забезпечення для перехоплення пакетів відкриває цифрову оболонку, щоб показати вам, які саме дані його перенасичують, звідки вони походять і чи містять вони шкідливі корисні навантаження. Воно долає розрив між базовим моніторингом безперебійної роботи та глибоким, практичним мережевим аналізом.

Аналізатор NetFlow від ManageEngine

ManageEngine NetFlow Analyzer – це інструмент аналізу мережевого трафіку, який надає організаціям можливості перевірки пакетів. Інструмент використовує протоколи NetFlow, sFlow, J-Flow та IPFIX для збору та аналізу даних мережевого трафіку.

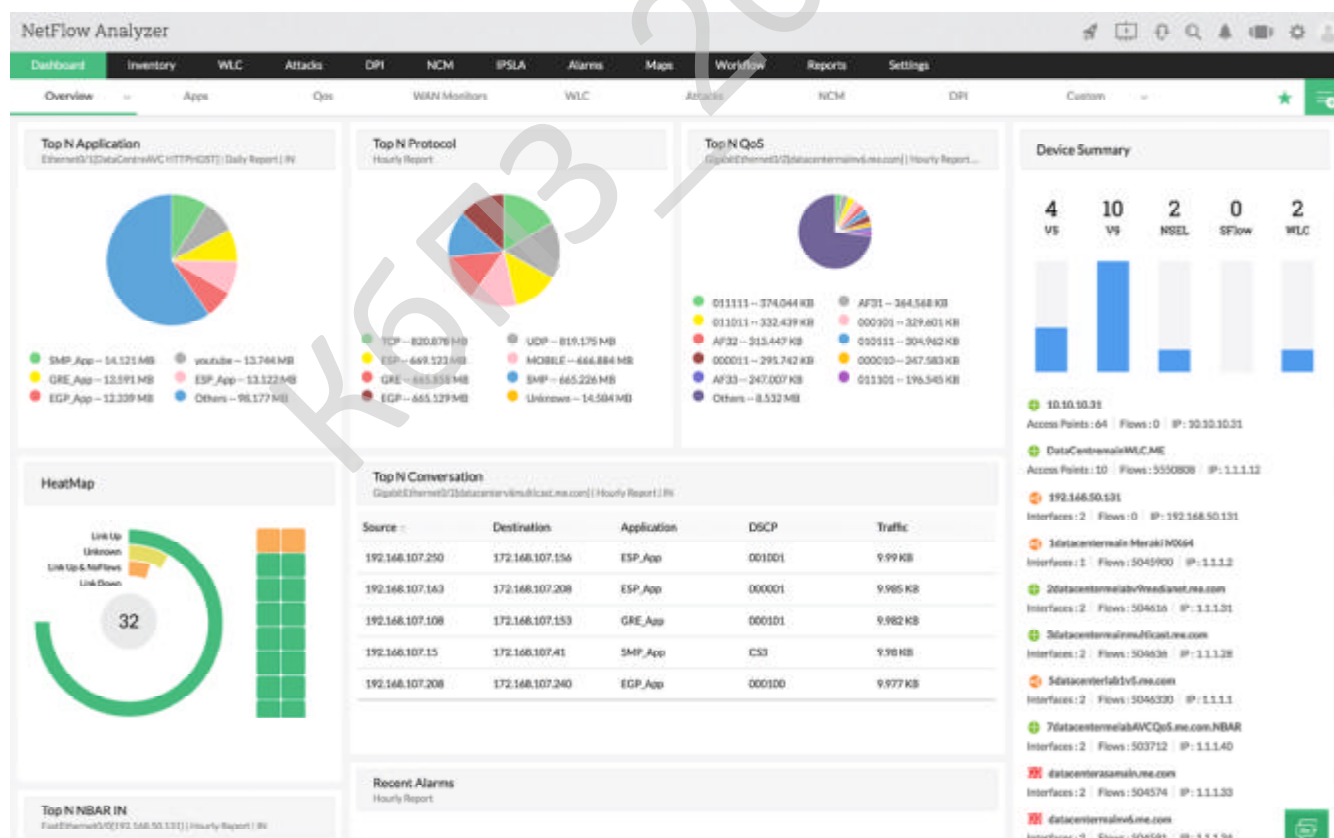


Рисунок 2.1 – Інтерфейс користувача ManageEngine NetFlow Analyzer

Цей інструмент надає організаціям можливість переглядати мережевий трафік у режимі реального часу та дозволяє їм контролювати, аналізувати та керувати мережевою активністю. Продукти ManageEngine розроблені, щоб допомогти організаціям спростити та оптимізувати процеси управління ІТ. Вони забезпечують єдине уявлення про ІТ-інфраструктуру, що дозволяє організаціям швидко виявляти та вирішувати проблеми, оптимізувати продуктивність та забезпечувати безпеку своїх ІТ-систем.

Paessler PRTG

Paessler PRTG – це комплексний інструмент моніторингу мережі, який забезпечує видимість стану та продуктивності ІТ-інфраструктури в режимі реального часу.

Він включає різні функції, такі як моніторинг різних мережевих пристроїв, використання пропускну здатності, хмарні сервіси, віртуальні середовища, програми тощо.

PRTG використовує перехоплення пакетів для виконання глибокого аналізу пакетів та звітності. Він також підтримує різні опції сповіщень, звітності та функції оповіщення, щоб адміністратори були в курсі стану мережі та потенційних проблем.

Wireshark

Wireshark – це програмний інструмент з відкритим кодом для аналізу мережевих протоколів, який використовується для моніторингу, усунення несправностей та аналізу мережевого трафіку. Він надає детальний огляд мережевих пакетів, включаючи їхні заголовки та корисні навантаження, що дозволяє користувачам бачити, що відбувається в їхній мережі.

Wireshark використовує графічний інтерфейс користувача, який забезпечує легку навігацію та фільтрацію захоплених пакетів, що робить його доступним для користувачів з різним рівнем технічних навичок. Крім того, він підтримує широкий спектр протоколів і має можливість декодувати та перевіряти численні типи даних.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

SolarWinds

Монітор продуктивності мережі SolarWinds (NPM) надає можливості глибокої перевірки та аналізу пакетів для моніторингу та усунення несправностей мережі.

NPM використовує передові алгоритми та протоколи для захоплення, декодування та аналізу мережевих пакетів у режимі реального часу, надаючи інформацію про моделі мережевого трафіку, використання пропускну здатності та продуктивність програм.

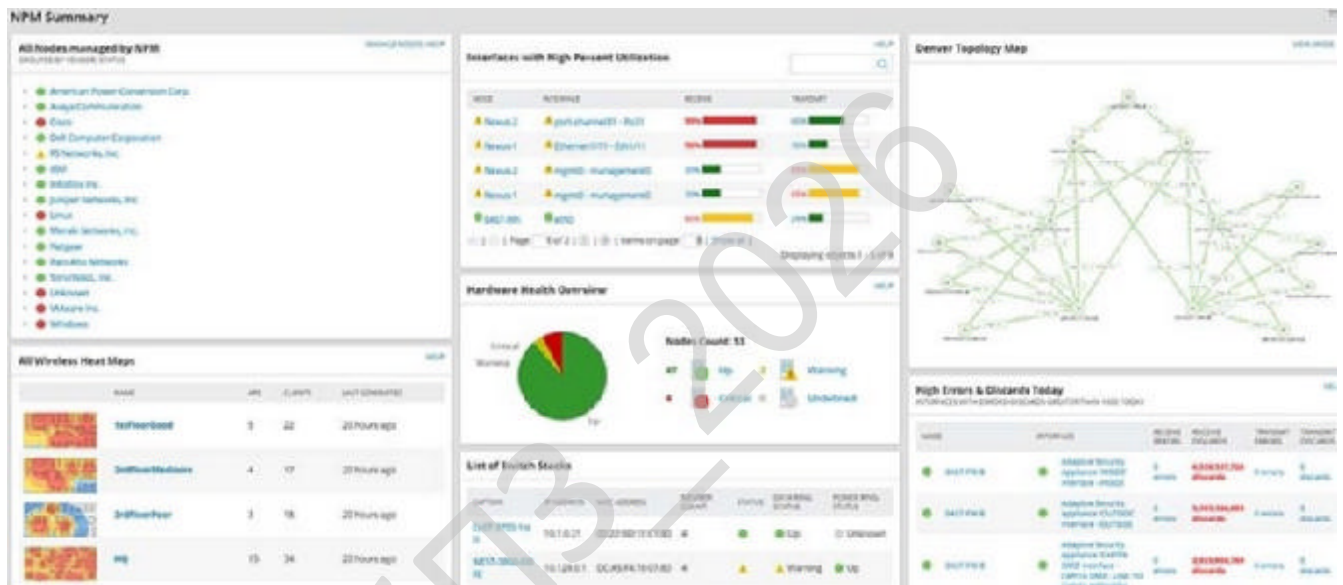


Рисунок 2.2 – Інтерфейс користувача SolarWinds

NPM – це комплексне рішення для мережевих адміністраторів та IT-фахівців, які хочуть глибше зрозуміти поведінку та продуктивність своєї мережі.

nDPI

NTop надає мережевим адміністраторам інструменти для моніторингу мережевого трафіку та продуктивності, включаючи захоплення пакетів, запис трафіку, мережеві зонди, аналіз трафіку та перевірку пакетів. Можливості DPI NTop базуються на nDPI, бібліотеці з відкритим кодом та розширюваній.

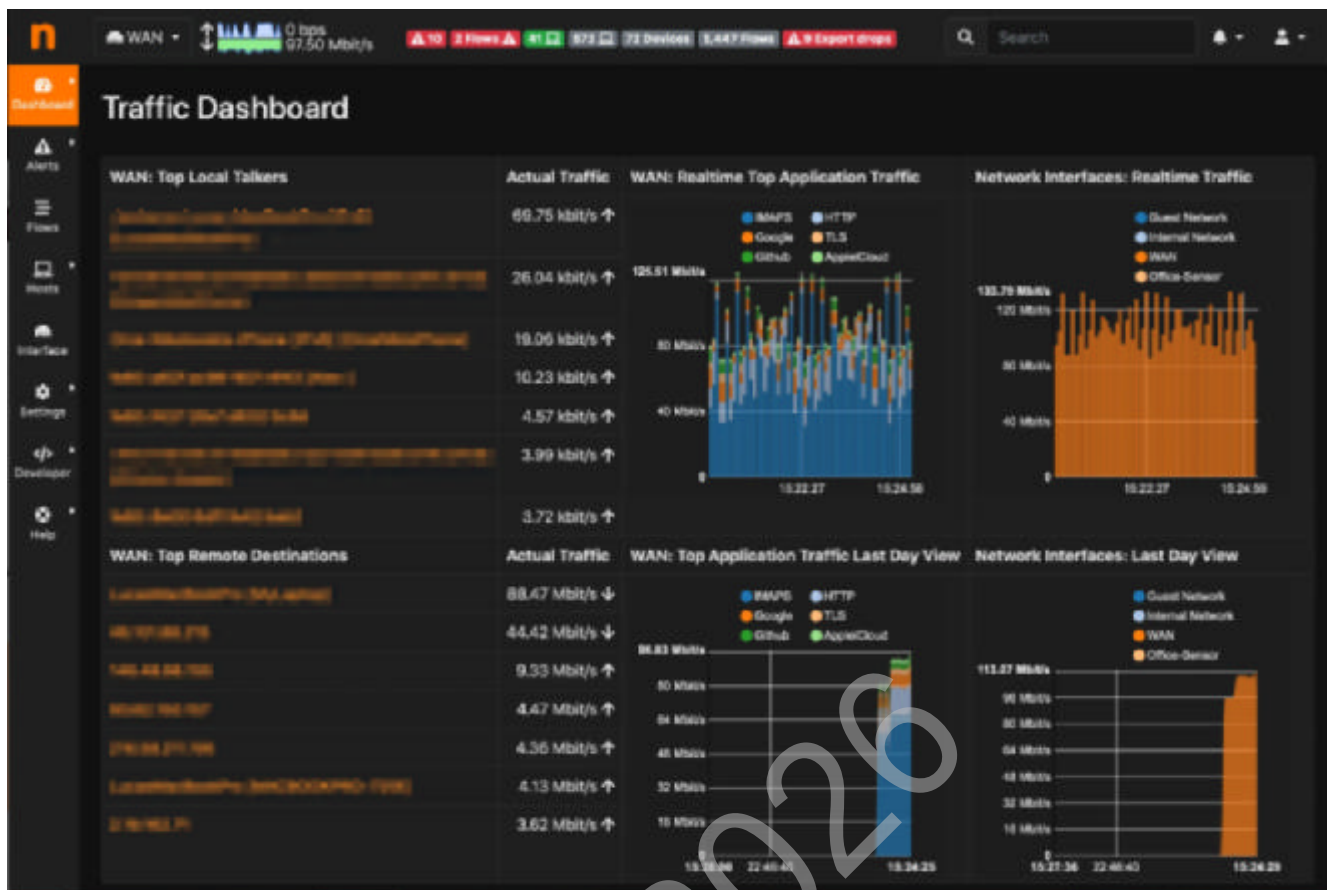


Рисунок 2.3 – Інтерфейс користувача nDPI

nDPI підтримує виявлення понад 500 різних протоколів і сервісів, а його архітектура розроблена для легкого розширення, що дозволяє користувачам додавати підтримку нових протоколів і сервісів.

Однак, nDPI – це лише бібліотека, і її необхідно використовувати разом з іншими програмами, такими як nTopng та nProbe Cento, для створення правил та вжиття заходів щодо мережевого трафіку.

Netify DPI

Netify DPI – це технологія перевірки пакетів, розроблена для забезпечення безпеки та оптимізації мережі. Інструмент має відкритий вихідний код і може бути розгорнутий на різних пристроях, від невеликих вбудованих систем до великої мережевої інфраструктури backend.

Він перевіряє мережеві пакети на рівні додатків, щоб забезпечити

видимість мережевого трафіку та моделей використання. Це допомагає організаціям виявляти загрози безпеці, контролювати продуктивність мережі та забезпечувати дотримання мережевих політик.

Як працює глибока перевірка пакетів?

Глибока перевірка пакетів (DPI) – це складний метод аналізу мережевого трафіку. Зазвичай він реалізується за допомогою спеціального пристрою або програмного компонента, який інтегрується в мережевий шлях. Основний процес DPI включає кілька ключових етапів для досягнення своїх цілей:

- Захоплення даних: Система DPI спочатку захоплює пакети даних, що проходять мережею. Це може бути зроблено безпосередньо або поза мережею.

- Декодування та підготовка даних: Після захоплення кожен пакет декодується. Це включає розбір різних шарів пакета, від мережевих заголовків до заголовків прикладного рівня та, що найважливіше, фактичного корисного навантаження даних. Система реконструює потік даних, щоб зрозуміти контекст зв'язку.

- Класифікація трафіку та поглиблений аналіз контенту: Після декодування система DPI виконує початкову класифікацію трафіку, наприклад, ідентифікуючи його як електронну пошту, передачу файлів або певні програми на основі номерів портів. Після цього відбувається більш детальний аналіз вмісту та контексту пакета.

Саме тут вступають у гру специфічні методи DPI:

- Аналіз на основі сигнатур: цей метод порівнює дані в пакетах з регулярно оновлюваною базою даних відомих шкідливих сигнатур. Ці сигнатури є шаблонами, пов'язаними з вірусами, шкідливим програмним забезпеченням, спробами вторгнення або іншими специфічними атаками.

- Поведінковий аналіз: Замість пошуку лише відомих закономірностей, цей метод встановлює базову лінію нормальної поведінки мережі для користувачів, програм і пристроїв. Потім він відстежує трафік на наявність відхилень, незвичайних закономірностей або підозрілої активності, яка може

свідчити про невідому загрозу, експлойт нульового дня або порушення політик.

– Аналіз та валідація протоколів: цей метод ретельно перевіряє мережевий трафік, щоб переконатися, що він відповідає очікуваним стандартам та специфікаціям використовуваних протоколів. Він може виявляти спотворені пакети, зловживання протоколом, спроби використання вразливостей протоколу або несанкціоноване тунелювання протоколів.

– Перевірка корисного навантаження: це передбачає безпосередню перевірку корисного навантаження даних у пакетах. Це не окремий метод, а скоріше базова можливість, що використовується іншими методами аналізу.

– Застосування політик та дії: На основі результатів етапів аналізу та попередньо визначених правил і політик, встановлених мережевими адміністраторами, система DPI вживає відповідних заходів. Це може включати дозвіл, блокування, фільтрацію, сповіщення, ведення журналу, обмеження швидкості або карантин.

2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування

Як мова програмування обрана Python. Python – високорівнева мова програмування загального призначення з акцентом на продуктивність розроблювача й читаність коду. Синтаксис ядра Python мінімалістичний. У той же час стандартна бібліотека включає великий обсяг корисних функцій.

Python підтримує кілька парадигм програмування, у тому числі структурне, об'єктно-орієнтоване, функціональне, імперативне й аспектно-орієнтоване. Основні архітектурні риси – динамічна типізація, автоматичне керування пам'яттю, повна інтроспекція, механізм обробки виключень, підтримка багатопоточні обчислень і зручні високорівневі структури даних. Код у Python організовується у функції й класи, які можуть поєднуватися в модулі (які у свою чергу можуть бути об'єднані в пакети).

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		13

Еталонною реалізацією Python є інтерпретатор CPython, що підтримує більшість активно використовуваних платформ. Він поширюється вільно під дуже ліберальною ліцензією, що дозволяє використовувати його без обмежень у будь-яких застосунках, включаючи пропрієтарні. Є реалізації інтерпретаторів для JVM (з можливістю компіляції), MSIL (з можливістю компіляції), LLVM і інших. Проект PyPy пропонує реалізацію Python на самому Python, що зменшує витрати на зміни мови й постановку експериментів над новими можливостями.

Python – мова програмування, що активно розвивається, нові версії (з додаванням/зміною мовних властивостей) виходять приблизно раз у два з половиною року. Внаслідок цього й деяких інших причин на Python відсутні ANSI, ISO або інші офіційні стандарти, їхню роль виконує CPython.

Python портований і працює майже на всіх відомих платформах – від КПК до мейнфреймів. Існують порти під Microsoft Windows, практично всі варіанти UNIX (включаючи FreeBSD і Linux), Plan 9, Mac OS і Mac OS X, iPhone OS 2.0 і вище, Palm OS, OS/2, Amiga, AS/400 і навіть OS/390, Symbian і Android.

При цьому, на відміну від багатьох портуємих систем, для всіх основних платформ Python має підтримку характерних для даної платформи технологій (наприклад, Microsoft COM/DCOM). Більше того, існує спеціальна версія Python для віртуальної машини Java – Jython, що дозволяє інтерпретаторові виконуватися на будь-якій системі, що підтримує Java, при цьому класи Java можуть безпосередньо використовуватися з Python й навіть бути написаними на Python. Також кілька проектів забезпечують інтеграцію із платформою Microsoft .NET, основні з яких – IronPython і Python.Net.

Python підтримує динамічну типізацію, тобто тип змінної визначається тільки під час виконання. Тому замість «присвоювання значення змінної» краще говорити про «зв'язування значення з деяким ім'ям». У Python є убудовані типи: бульові, рядки, Unicode-рядки, цілі числа довільної точності, числа із плаваючою комою, комплексні числа й деякі інші. З колекцій Python підтримує кортежі (*tuples*), списки, словники (асоціативні масиви) і, починаючи з версії 2.4, безлічі.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

Всі значення в Python є об'єктами, у тому числі функції, методи, модулі, класи. Додати новий тип можна або написавши клас (class), або визначивши новий тип у модулі розширення (наприклад, написаному мовою C). Система класів підтримує спадкування (одиначне й множинне) і метапрограмування. Можливе спадкування від більшості убудованих типів і типів розширень.

Всі об'єкти діляться на посилальні й атомарні. До атомарного ставляться int, long, complex і деякі інші. При присвоюванні атомарних об'єктів копіюється їхнє значення, у той час як для посилальних копіюється тільки покажчик на об'єкт, таким чином, обидві змінні після присвоювання використовують те саме значення. Посилальні об'єкти бувають змінювані й незмінні. Наприклад, рядки й кортежі є незмінними, а списки, словники й багато інших об'єктів – змінюваними. Кортеж у Python є, по суті, незмінним списком. У багатьох випадках кортежі працюють швидше списків, тому якщо ви не плануєте змінювати послідовність, то краще використовувати саме їх.

Мова має чіткий і послідовний синтаксис, продуману модульність й масштабованість, завдяки чому вихідний код написаних на Python програм легко читаємий.

Python – стабільна й розповсюджена мова. Він використовується в багатьох проектах і в різних якість: як основна мова програмування або для створення розширень і інтеграції застосунків. На Python реалізоване велика кількість проектів, також він активно використовується для створення прототипів майбутніх програм. Python використовується в багатьох великих компаніях.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускню кваліфікаційну роботу за першим (бакалаврським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

В процесі розробки випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти необхідно виконати наступний обсяг роботи:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи кібербезпеки контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи кібербезпеки в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформулювати висновки про виконаний обсяг робіт та одержані результати.

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Глибока перевірка пакетів (DPI) залишається критично важливою методикою для аналізу мережевого трафіку, що дозволяє комплексно досліджувати як заголовки пакетів, так і вміст корисного навантаження для забезпечення безпеки, дотримання політик та управління трафіком. Оскільки мережеві загрози стають все більш складними, особливо через атаки соціальної інженерії на основі глибоких фейків, існує гостра потреба в розширенні можливостей DPI шляхом розробки інтелектуальних брандмауерів, які інтегрують машинне навчання (ML) для виявлення загроз у режимі реального часу.

Ринок глибокої перевірки пакетів переживає стрімке та стійке зростання, оскільки організації по всьому світу стикаються з безпрецедентним зростанням складності мережевого трафіку та складними кіберзагрозами. Технологія глибокої перевірки пакетів (DPI), яка аналізує частину даних та заголовків мережевого пакета під час його проходження через точку перевірки, перетворилася на незамінний інструмент для підприємств та мережевих операторів, які прагнуть отримати повну видимість своєї мережевої інфраструктури. У 2025 році середня корпоративна мережа обробляла понад 4,8 екзабайта даних на місяць, що підкреслює необхідність розширених можливостей аналізу трафіку. Поширення хмарних додатків, віддалених працівників та пристроїв з підтримкою Інтернету речей значно розширило поверхню атаки, змушуючи організації використовувати рішення DPI як першу лінію захисту. Уряди Північної Америки, Європи та Азіатсько-Тихоокеанського регіону запровадили суворі правила конфіденційності даних та безпеки мережі, включаючи оновлення таких фреймворків, як GDPR, CCPA та національні

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

мандати кібербезпеки, що ще більше прискорює впровадження підприємствами. Перехід до інфраструктури 5G призвів до нових моделей трафіку та вимог до затримки, які застарілі інструменти моніторингу мережі не можуть адекватно врахувати, позиціонуючи DPI як критично важливий інструмент для управління мережею наступного покоління. Телекомунікаційні оператори є особливо активними користувачами, використовуючи DPI для забезпечення дотримання політик якості обслуговування (QoS), управління розподілом пропускної здатності та монетизації мережевих даних за допомогою послуг з доданою вартістю. Ринок також отримує вигоду від досягнень у машинному навчанні та штучному інтелекті, які інтегруються в платформи DPI, що дозволяє проводити поведінкову аналітику в режимі реального часу та автоматизовано реагувати на загрози на швидкостях ліній зв'язку понад 400 Гбіт/с. Як результат, інвестиції в технологію глибокої перевірки пакетів продовжують прискорюватися в BFSI, уряді, охороні здоров'я, а також у сфері ІТ та телекомунікацій, зміцнюючи позитивні довгострокові перспективи ринку до 2034 року.

Глибока перевірка пакетів (DPI) – це вдосконалений метод фільтрації мережевого трафіку, який аналізує вміст даних мережевих пакетів на прикладному рівні (рівень 7) моделі OSI, виходячи далеко за рамки аналізу заголовків, що виконується звичайними брандмауерами. Системи DPI можуть ідентифікувати, класифікувати та блокувати або перенаправляти мережеві пакети на основі даних корисного навантаження, підписів протоколів або шаблонів, специфічних для програми, що дозволяє детально застосовувати політики. У 2025 році провідні платформи DPI від таких постачальників, як Cisco та Palo Alto Networks, здатні перевіряти зашифровані потоки трафіку за допомогою дешифрування SSL/TLS з пропускною здатністю понад 100 Гбіт/с. Це робить DPI унікально потужним для таких випадків використання, як виявлення та запобігання вторгненням, законне перехоплення, фільтрація контенту та формування трафіку з урахуванням програм у мережах корпоративного та операторського класу.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		18

Зростання кіберзагроз та поширення програм-вимагачів

Експоненціальне зростання кібератак стало найпотужнішим рушієм попиту на ринку глибокої перевірки пакетів даних. Згідно зі звітами з кібербезпеки, опублікованими на початку 2026 року, очікується, що глобальні витрати на кіберзлочинність перевищать 10,5 трильйонів доларів США щорічно до 2026 року, порівняно з 8 трильйонами доларів США у 2023 році. Операції програм-вимагачів як послуги (RaaS) зросли більш ніж на 62% у річному обчисленні, з дедалі більшою частотою та складністю атакуючи критично важливу інфраструктуру, мережі охорони здоров'я та фінансові установи. Технологія DPI має унікальні можливості для виявлення та нейтралізації передових загроз шляхом перевірки зашифрованих корисних даних у режимі реального часу, виявлення шаблонів трафіку систем управління та контролю (C2) та блокування горизонтального руху в корпоративних мережах до того, як пошкодження поширяться. Провідні постачальники, включаючи Palo Alto Networks та Fortinet, інтегрували механізми DPI з потоками інформації про загрози, що оновлюються з інтервалом менше секунди, що дозволяє проактивно усувати вразливості нульового дня. Зростаюче впровадження багатовекторних стратегій атак, що поєднують фішинг, компрометацію ланцюгів поставок та мережеву експлуатацію, зробило традиційні підходи до захисту периметра неадекватними, що змусило організації з усіх вертикалей інвестувати в детальні рішення для забезпечення видимості мережі, засновані на DPI. Підприємства з кількістю співробітників понад 5000 повідомили про 38% збільшення охоплення розгортанням DPI між 2023 і 2025 роками, що відображає зростаючу роль технології як ключового елемента багаторівневої архітектури кібербезпеки.

Розгортання мережі 5G та поширення Інтернету речей

Глобальне розгортання мереж 5G фундаментально трансформує ринок глибокої перевірки пакетів, створюючи як нові можливості, так і нові виклики для видимості та безпеки мережі. До кінця 2025 року в усьому світі було активних понад 2,8 мільярда підключень 5G, а згідно з даними GSMA Intelligence,

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

до 2029 року ця кількість, за прогнозами, перевищить 5,5 мільярда. Дезагрегована, програмно-визначена архітектура основних мереж 5G, що характеризується розділенням мережі, мобільними периферійними обчисленнями (MEC) та віртуалізацією мережевих функцій (NFV), генерує значно складніші та неоднорідні потоки трафіку, ніж застарілі мережі 4G LTE, вимагаючи платформ DPI, здатних працювати з пропускнуою здатністю терабіт на секунду. Одночасно глобальна встановлена база пристроїв Інтернету речей досягла 18,8 мільярда одиниць у 2025 році та, за прогнозами, зросте до понад 30 мільярдів до 2030 року, що представить мільярди нових, часто погано захищених кінцевих точок для корпоративних та операторських мереж. Рішення DPI мають вирішальне значення для виявлення аномальної поведінки пристроїв Інтернету речей, забезпечення дотримання політик мікросегментації та запобігання атакам ботнетів на основі Інтернету речей, таким як варіанти Mirai, що використовують неадекватну автентифікацію пристроїв. У 2025 році Nokia та Huawei випустили спеціалізовані модулі DPI, орієнтовані на 5G, розроблені для безперешкодної інтеграції з їхніми відповідними портфоліо Open RAN та основних мереж, що сигналізує про структурний зсув у тому, як технологія DPI постачається та використовується телекомунікаційними операторами по всьому світу. Інтеграція DPI з інтерфейсами сервісної архітектури (SBA) в автономних мережах 5G (SA) також дозволяє операторам створювати мережеві сегменти, що враховують політики та чутливі до додатків, які можуть динамічно адаптуватися до умов трафіку в режимі реального часу, відкриваючи нові потоки доходів, що виходять за рамки базового підключення.

Суворі вимоги до дотримання нормативних вимог та управління даними

Регуляторні вимоги є потужним та довговічним попутним вітром для ринку глибокої перевірки пакетів, змушуючи організації у фінансовому секторі, охороні здоров'я, телекомунікаціях та державному секторі впроваджувати можливості перевірки трафіку як передумову для дотримання вимог.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

Запровадження GDPR у Європейському Союзі, де штрафи сягають 4% від світового річного обороту, спонукало підприємства впроваджувати моніторинг витоку даних на основі DPI та виявлення персональної інформації (PII) по всьому периметру своєї мережі. У Сполучених Штатах галузеві рамки, включаючи HIPAA для охорони здоров'я, PCI DSS для даних платіжних карток та NIST SP 800-207 для архітектури нульової довіри, неявно вимагають можливостей аналізу мережевого трафіку, які надають платформи DPI. Впровадження Директиви ЄС NIS2, яка набула чинності в жовтні 2024 року та розширила сферу діяльності секторів критичної інфраструктури, що підлягають обов'язковому звітуванню про інциденти та контролю безпеки, спричинило хвилю закупівель DPI серед європейських комунальних підприємств, транспортних операторів та постачальників цифрової інфраструктури. В Азіатсько-Тихоокеанському регіоні Закон Китаю про кібербезпеку та Закон про захист персональної інформації (PIPL), а також Закон Індії про захист цифрових персональних даних 2023 року створюють попит на рішення DPI, здатні забезпечувати виконання вимог щодо локалізації даних та моніторингу транскордонних потоків даних, що зумовлено дотриманням вимог. Уряди країн регіону Ради співробітництва арабських держав Перської затоки (GCC) також прийняли національні правила кібербезпеки, які вимагають від операторів зв'язку розгортати законні рішення для перехоплення, що базуються на технології DPI, при цьому Уряд Саудівської Аравії з питань основних засобів контролю за кібербезпекою та Національна стратегія кібербезпеки ОАЕ виступають ключовими законодавчими каталізаторами на Близькому Сході.

Інтеграція штучного інтелекту та машинного навчання з платформами DPI

Конвергенція штучного інтелекту та машинного навчання з технологією DPI стає однією з найбільш трансформаційних тенденцій на ринку, що значно підвищує точність, швидкість та масштабованість аналізу мережевого трафіку. Традиційні підходи DPI на основі сигнатур намагаються встигати за сучасними

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		21

зашифрованими загрозами та методами обфускації додатків; платформи DPI з доповненням ШІ усувають це обмеження, застосовуючи поведінкову аналітику, виявлення аномалій та моделі прогнозової класифікації до потоків трафіку в режимі реального часу. У 2025 році постачальники, включаючи Cisco, IBM та Trend Micro, випустили нові оновлення платформи DPI, які включають механізми кореляції загроз на основі моделей великих мов програмування (LLM), здатні знизити рівень хибнопозитивних сповіщень до 47% порівняно з системами на основі правил, одночасно скорочуючи середній час виявлення (MTTD) з годин до менш ніж 90 секунд. Інтеграція ШІ також дозволяє автоматизовану адаптацію політик, коли системи DPI динамічно коригують класифікацію трафіку та правила забезпечення дотримання правил у відповідь на спостережувану поведінку мережі без втручання людини, зменшуючи операційне навантаження на команди центру операцій безпеки (SOC). Хмарні рішення DPI, що використовують контейнерні архітектури мікросервісів, забезпечують горизонтальну масштабованість, дозволяючи постачальникам послуг розширювати можливості інспекції на вимогу без виділення додаткового спеціалізованого обладнання. Галузеві аналітики прогнозують, що до 2027 року понад 65% нових розгорнутих рішень DPI включатимуть певну форму класифікації трафіку на основі штучного інтелекту, порівняно з приблизно 28% у 2024 році, що являє собою фундаментальну еволюцію можливостей та ціннісної пропозиції технології. Ця тенденція особливо виражена серед постачальників гіпермасштабованих хмарних послуг та великих телекомунікаційних операторів, які прагнуть використовувати мережеві дані як джерело конкурентної розвідки та диференціації послуг.

Аналіз ринку DPI за компонентами

У 2025 році сегмент програмного забезпечення займав найбільшу частку ринку DPI за компонентами, становлячи 42,3% світового доходу (5,4 млрд доларів США), що відображає ширший галузевий перехід від спеціалізованих апаратних пристроїв до гнучких програмно-визначених платформ перевірки, які

можна розгорнути у віртуальних та хмарних середовищах. Програмні рішення DPI пропонують значні переваги з точки зору гнучкості розгортання, вартості володіння та частоти оновлення порівняно з їхніми апаратними аналогами. Провідні програмні платформи від Palo Alto Networks, Fortinet та IBM Security включають модульні механізми DPI, які можна оновлювати за допомогою бездротових (OTA) сигнатур та оновлення моделей штучного інтелекту, що дозволяє організаціям підтримувати захист від нових загроз без циклів заміни фізичного обладнання. Прогнозується, що сегмент програмного забезпечення зростатиме зі середньорічним темпом зростання (CAGR) 6,8% з 2026 по 2034 рік, що є найвищим показником серед усіх категорій компонентів, завдяки прискоренню міграції підприємств до хмарних технологій, розвитку хмарних архітектур периферійних служб безпеки (SSE) та розширення розгортання програмно-визначених глобальних мереж (SD-WAN), які вимагають інтегрованих можливостей DPI для маршрутизації трафіку з урахуванням додатків. Впровадження підприємствами моделей ліцензування програмного забезпечення DPI на основі підписки, які узгоджують витрати з фактичним використанням та включають постійні оновлення інформації про загрози, також сприяє значному зростанню доходів у цьому підсегменті протягом прогнозованого періоду.

У 2025 році сегмент апаратного забезпечення становив приблизно 35,4% доходів світового ринку DPI і охоплює спеціалізовані пристрої DPI, карти перевірки на основі програмованих польовими елементами вентиляльних матриць (FPGA) та спеціально розроблені мережеві зонди, розроблені для середовищ з високою пропускну здатністю. Апаратна DPI залишається кращим вибором для операторів телекомунікацій, точок обміну інтернет-трафіком та великих центрів обробки даних, де стійка перевірка на швидкості лінії від 100 Гбіт/с до 400 Гбіт/с є невід'ємною технічною вимогою, яку програмні рішення поки що не можуть надійно задовольнити без прискорення розвантаження. Постачальники, включаючи Cisco, Juniper Networks, Nokia та Huawei, продовжують інвестувати в DPI ASIC наступного покоління та

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

програмовані мікросхеми переадресації, які поєднують глибоку перевірку з субмікросекундною затримкою. Очікується, що сегмент апаратного забезпечення зростатиме зі середньорічним темпом зростання 4,6% до 2034 року, що дещо нижче, ніж у програмного забезпечення, оскільки підприємства все більше переходять до віртуальних та хмарних впроваджень DPI, тоді як розгортання центрів обробки даних операторського класу та високопродуктивних центрів обробки даних продовжує підтримувати попит на фізичні пристрої. Сегмент послуг, який включає професійні послуги, такі як інтеграція, консалтинг та навчання, а також керовані послуги DPI, займав частку приблизно 22,3% у 2025 році та, за прогнозами, зростатиме зі середньорічним темпом зростання 5,8% , що підтримується зростаючим попитом з боку середніх підприємств, яким бракує власної експертизи в галузі DPI, та розширенням пропозицій постачальників послуг керованої безпеки (MSSP), що включають DPI як компонент керованої послуги.

Аналіз ринку DPI за застосуванням

Виявлення та запобігання вторгненням становили найбільший сегмент застосування на ринку DPI у 2025 році, забезпечуючи приблизно 31,8% світового доходу (4,1 мільярда доларів США), що було зумовлено невпинною ескалацією складних кібератак, спрямованих на корпоративні та урядові мережі. Системи виявлення та запобігання вторгненням (IDPS) на основі DPI забезпечують детальну перевірку корисних даних пакетів для виявлення шкідливих сигнатур, аномалій протоколів та поведінкових індикаторів компрометації (IoC), які обходять традиційні підходи до виявлення на основі брандмауерів та сигнатур. Зростаюча складність передових стійких загроз (APT) та кібератак, що спонсоруються державами, зробила IDPS з додаткового засобу контролю безпеки критично важливим засобом для організацій у всіх секторах. Організації охорони здоров'я, фінансові установи та оператори критичної інфраструктури повідомили про сукупне збільшення бюджетів на закупівлі IDPS на основі DPI на 51% у період з 2023 по 2025 рік. Інтеграція DPI з платформами управління інформацією

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

та подіями безпеки (SIEM), інструментами оркестрації безпеки, автоматизації та реагування (SOAR), а також розширеними рішеннями виявлення та реагування (XDR) ще більше підвищує цінність сегмента застосувань виявлення та запобігання вторгненням, забезпечуючи скоординоване, автоматизоване реагування на загрози в усій екосистемі безпеки. Зростаюче впровадження платформ відеоспостереження та аналітики безпеки в корпоративних середовищах також створює додатковий попит на рішення DPI, які можуть контролювати та захищати потоки відеотрафіку з високою пропускнуою здатністю та чутливістю до затримки, що генеруються цими системами.

Управління продуктивністю мережі становило приблизно 22,7% світового доходу від додатків DPI у 2025 році, що є критичним випадком використання для постачальників телекомунікаційних послуг, інтернет-провайдерів (ISP) та великих мережевих команд підприємств, які прагнуть оптимізувати якість обслуговування (QoE) для критично важливих для бізнесу додатків. DPI забезпечує детальну видимість складу трафіку на рівні додатків, дозволяючи мережевим операторам розрізняти чутливий до затримки трафік уніфікованих комунікацій та дані масової передачі файлів, а також відповідно застосовувати диференційовані політики якості обслуговування (QoS). Вибухове зростання платформ відеоконференцій у реальному часі, таких як Microsoft Teams, Cisco Webex та Zoom, які споживали приблизно 42% пропускнуї здатності корпоративної WAN у 2025 році, значно підвищило стратегічну важливість моніторингу продуктивності додатків та інженерії трафіку на основі DPI. Запобігання втраті даних (DLP) становило третій за величиною сегмент додатків, захопивши приблизно 18,4% доходу ринку у 2025 році, з високим попитом з боку фінансових послуг, охорони здоров'я та державного сектору, де несанкціоноване витік даних має серйозні регуляторні та репутаційні наслідки. Рішення DLP на основі DPI можуть перевіряти зашифровані потоки трафіку на наявність конфіденційних шаблонів даних, включаючи особисту ідентифікаційну інформацію, номери платіжних карток та захищену медичну інформацію (PHI),

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

забезпечуючи більш комплексні можливості захисту даних, ніж підходи DLP лише на кінцевих точках. Дотримання нормативних вимог становило приблизно 14,2% доходу додатків у 2025 році, тоді як інші додатки, включаючи законне перехоплення, батьківський контроль та фільтрацію контенту, разом становили решту 12,9%. Прогнозується, що сегмент дотримання нормативних вимог зареєструє найвищий середньорічний темп зростання (CAGR) на рівні 7,1% до 2034 року, оскільки глобальний регуляторний ландшафт продовжує посилюватися. Сектор технологій розпізнавання облич також все більше інтегрується з інфраструктурою DPI для забезпечення дотримання політики на основі ідентифікації в середовищах з високим рівнем безпеки.

Аналіз ринку DPI за режимом розгортання

Локальне розгортання становило більший сегмент ринку DPI за режимом розгортання у 2025 році, займаючи приблизно 57,9% світового доходу, оскільки великі підприємства, державні установи та оператори телекомунікацій із суворими вимогами до суверенітету даних, затримки та відповідності продовжують віддавати перевагу розгортанню інфраструктури DPI у власних центрах обробки даних та мережевих периметрах. Локальні рішення DPI пропонують повний контроль над обробкою даних, журналами трафіку та забезпеченням дотримання політик без залежності від зовнішнього мережевого підключення, що робить їх особливо придатними для класифікованих урядових мереж, фінансових установ першого рівня та організацій охорони здоров'я, на які поширюються вимоги HIPAA та аналогічні вимоги щодо локалізації даних. Прогнозується, що сегмент локальних рішень зростатиме зі середньорічним темпом зростання 4,8% з 2026 по 2034 рік, що є стабільним, хоча й дещо нижчим темпом порівняно з хмарним сегментом, оскільки фундаментальна вимога до спеціалізованого високопродуктивного обладнання для перевірки в основних мережевих середовищах підтримує попит, навіть коли міграція до хмари прискорюється в інших IT-навантаженнях. Сегмент продовжує отримувати вигоду від розгортання пристроїв DPI наступного покоління з покращеною

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		26

пропускною здатністю та нижчими витратами на перевірку біта.

Сегмент розгортання хмарних технологій зайняв приблизно 42,1% доходів світового ринку DPI у 2025 році та є найшвидше зростаючим сегментом, який, за прогнозами, зростатиме зі середньорічним темпом зростання (CAGR) 7,4% до 2034 року. Хмарні рішення DPI все частіше постачаються як частина ширших архітектур хмарних сервісів безпеки на периферії (SSE), безпечного доступу на периферії (SASE) та брандмауера як послуги (FWaaS), що пропонуються такими постачальниками, як Palo Alto Networks (Prisma Access), Zscaler та Cisco (Umbrella). Перехід до моделей віддаленої та гібридної роботи, який різко прискорився під час пандемії COVID-19 і з того часу став постійною рисою корпоративної робочої культури, фундаментально змінив моделі мережевого трафіку, спрямовуючи більшу частину корпоративного трафіку даних через загальнодоступний Інтернет, а не через контрольовані периметри корпоративної мережі. Цей перехід створив структурний попит на хмарні можливості DPI, які можуть перевіряти та захищати трафік незалежно від місцезнаходження користувача чи кінцевого пристрою. Малі та середні підприємства (МСП) представляють особливо динамічний сегмент покупців хмарних DPI, оскільки моделі ціноутворення на основі підписки усувають бар'єри капітальних витрат, пов'язані з локальним розгортанням обладнання. Зростаюча інтеграція рішень відеоаналітики з хмарними платформами безпеки також сприяє впровадженню хмарних DPI серед організацій, які розгортають підключені до мережі системи камер, що вимагають аналізу трафіку в режимі реального часу та виявлення аномалій. Очікується, що до 2027 року хмарне розгортання перевершить локальне розгортання як домінуючий спосіб доставки для нових розгортань DPI, що являтиме собою фундаментальний структурний зсув на ринку.

Яка різниця між глибокою перевіркою пакетів та традиційним брандмауером?

Традиційні брандмауери працюють переважно на 3-му та 4-му рівнях моделі OSI, фільтруючи трафік на основі IP-адрес, портів та транспортних

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		27

протоколів, не перевіряючи фактичний вміст корисних навантажень пакетів. Глибока перевірка пакетів працює на 7-му рівні, аналізуючи повний вміст кожного пакета на рівні додатків, включаючи корисне навантаження даних, підписи додатків та контекст сеансу, що дозволяє набагато детальніше застосовувати політики та виявляти загрози. Наприклад, традиційний брандмауер може пропускати весь трафік на TCP-порті 443 (HTTPS), тоді як система DPI може розрізняти легітимний корпоративний SaaS-трафік, зашифровані комунікації командного програмного забезпечення та несанкціоновані завантаження хмарних сховищ, що проходять через той самий порт. У корпоративних середовищах у 2025 році брандмауери наступного покоління (NGFW) на основі DPI від таких постачальників, як Palo Alto Networks та Fortinet, досягають точності ідентифікації додатків, що перевищує 99,3%, що дозволяє здійснювати контроль доступу до мережі з нульовою довірою на основі ідентифікації додатків, а не лише на основі порту та протоколу.

Аналіз ринку DPI за розміром підприємства

У 2025 році великі підприємства становили домінуючий сегмент покупців на ринку DPI за розміром підприємств, на які припадало приблизно 67,2% від загального світового доходу (8,6 мільярда доларів США). Великі підприємства зазвичай експлуатують складні мережеві середовища з кількома сайтами, що охоплюють сотні локацій по всьому світу, що вимагає комплексного розгортання DPI на кількох мережевих рівнях, включаючи сегменти кампусів, філій, центрів обробки даних та глобальних мереж (WAN). Масштаб і складність великих корпоративних мереж у поєднанні зі значними бюджетами на ІТ-безпеку, які в середньому становили приблизно 18,4 мільйона доларів США на організацію у 2025 році для компаній з кількістю співробітників понад 10 000, дозволяють закуповувати складні, високопродуктивні платформи DPI від преміальних постачальників. Великі фінансові установи та глобальні технологічні компанії є одними з найбільших витратників на DPI на організацію, мотивовані подвійними імперативами захисту критично важливої інтелектуальної власності та

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

дотримання галузевих норм безпеки. Попит з боку великих підприємств також формується зростаючим впровадженням архітектур доступу до мережі з нульовою довірою (ZTNA), де DPI використовується як основний механізм для перевірки легітимності та вмісту кожної мережевої транзакції, незалежно від місцезнаходження джерела чи ідентифікаційних даних. Очікується, що сегмент великих підприємств зростатиме зі середньорічним темпом зростання (CAGR) на рівні 5,4% з 2026 по 2034 рік.

Сегмент малих та середніх підприємств (МСП) становив приблизно 32,8% ринку DPI за розміром підприємства у 2025 році та, як очікується, зростатиме зі швидшим середньорічним темпом зростання (CAGR) на рівні 6,8% до 2034 року, що відображає демократизацію передових можливостей мережевої безпеки завдяки хмарним та передплатним пропозиціям DPI. Історично склалося так, що висока капітальна вартість спеціалізованих пристроїв DPI та спеціалізований досвід, необхідний для налаштування та управління, обмежували впровадження DPI серед МСП найбільшими та найбільш свідомими до безпеки організаціями в сегменті. Однак поява хмарних платформ DPI, керованих послуг DPI від постачальників послуг з управління загрозами (MSSP) та інтегрованих можливостей DPI в уніфікованих пристроях управління загрозами (UTM) наступного покоління, орієнтованих на ринок МСП, значно знизил бар'єр входу. Зростаюча обізнаність про ризики кібербезпеки серед керівництва МСП, підкріплена гучними атаками програм-вимагачів на підприємства з кількістю співробітників менше 500, на які припадало понад 41% усіх інцидентів із програмами-вимагачами у 2025 році, призводить до значного зростання інвестицій у технології безпеки на рівні МСП. Урядові програми, включаючи портал ресурсів з кібербезпеки Адміністрації малого бізнесу США та посібник для малих і середніх підприємств Європейського агентства з кібербезпеки (ENISA) ЄС, також сприяють впровадженню DPI серед невеликих організацій як частини національних стратегій цифрової стійкості.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		29

Аналіз ринку DPI кінцевими користувачами

Сегмент кінцевих користувачів ІТ та телекомунікацій очолив ринок DPI у 2025 році, отримавши приблизно 28,6% світового доходу (3,7 мільярда доларів США), оскільки оператори зв'язку та інтернет-провайдери є найбільшими розгортачами технології DPI на рівні мережевої інфраструктури. Телекомунікаційні компанії використовують DPI для широкого спектру операційних цілей, включаючи дотримання законних вимог щодо перехоплення, управління даними абонентів, забезпечення дотримання політики трафіку, фільтрацію контенту та оптимізацію продуктивності мережі в своїх основних, агрегаційних та мережевих доменах доступу. Поточний перехід основних операторів у всьому світі до автономних (SA) мереж 5G створює значний попит на заміну та оновлення рішень DPI операторського класу, здатних обробляти різко збільшені обсяги трафіку, нижчі вимоги до затримки та складніші моделі трафіку, характерні для мереж 5G. У 2025 році оператори телекомунікацій разом представляли найбільшу щорічну категорію інвестицій в апаратне та програмне забезпечення DPI у світі, причому витрати на інфраструктуру перевірки трафіку на одного оператора коливалися від 45 мільйонів доларів до понад 300 мільйонів доларів для операторів першого рівня. Сегмент кінцевих користувачів BFSI (банківська справа, фінансові послуги та страхування) становив приблизно 21,3% доходу ринку у 2025 році, що зумовлено жорсткою потребою захищати цінні фінансові дані, дотримуватися нормативних актів, включаючи PCI DSS та SOX, та виявляти складні фінансові шахрайства в режимі реального часу. Фінансові установи впроваджують DPI разом із платформами поведінкової аналітики для виявлення внутрішніх загроз та атак захоплення облікових записів, які демонструють ледь помітні поведінкові сигнатури на мережевому рівні, невидимі для традиційних інструментів безпеки. Інтеграція DPI з системами автоматичного розпізнавання номерних знаків та інфраструктурою фізичної безпеки також набирає обертів у державному та транспортному секторах.

Сегмент кінцевих користувачів державних установ становив

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		30

приблизно 17,4% світового доходу ринку DPI у 2025 році та, як очікується, зростатиме зі середньорічним темпом зростання (CAGR) на рівні 6,1% до 2034 року, що зумовлено національними стратегіями кібербезпеки, ініціативами щодо захисту критичної інфраструктури та законними мандатами на перехоплення як у розвинених, так і в країнах, що розвиваються. Урядові установи на федеральному, штатному та місцевому рівнях впроваджують DPI як ключову технологію для захисту класифікованих мереж, захисту критичної інфраструктури, такої як електромережі та водоочисні споруди, та забезпечення дотримання національної політики кібербезпеки. Сегмент кінцевих користувачів охорони здоров'я становив приблизно 13,8% доходу ринку у 2025 році, зростаючи зі середньорічним темпом зростання на рівні 6,4%, що зумовлено швидкою цифровізацією медичного обслуговування, поширенням підключених медичних пристроїв (IoMT) та катастрофічними наслідками витоків даних у сфері охорони здоров'я, які лише у 2025 році розкрили понад 168 мільйонів записів пацієнтів у всьому світі. У 2025 році сегмент роздрібних кінцевих користувачів займав приблизно 8,6% ринкового доходу, причому його впровадження було зумовлене необхідністю захисту даних платіжних карток, забезпечення безпеки омніканальних платформ цифрової комерції та дотримання вимог стандарту PCI DSS. Інші галузі кінцевих користувачів, включаючи освіту, виробництво, енергетику та комунальні послуги, разом становили решту 10,3% ринкового доходу, при цьому очікується, що підсегмент енергетики та комунальних послуг продемонструє особливо сильне зростання, оскільки мережі операційних технологій (OT) та промислових систем управління (ICS) все більше підключаються до корпоративних IT-мереж, створюючи нові вразливості, які технологія DPI має всі можливості для усунення.

Як використовується глибока перевірка пакетів у мережах 5G?

У мережах 5G глибока перевірка пакетів відіграє вирішальну роль у забезпеченні контролю політик, класифікації трафіку та забезпеченні безпеки в дезагрегованих мережевих архітектурах, які є набагато складнішими, ніж

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		31

попередні покоління. Функції DPI вбудовані в основні функції мережі 5G, включаючи функцію площини користувача (UPF), яка відповідає за маршрутизацію, пересилання пакетів та забезпечення якості обслуговування (QoS) для всього трафіку користувачів в автономній архітектурі 5G. Постачальники телекомунікаційних послуг, такі як Nokia, Ericsson та Huawei, розробили модулі DPI, спеціально розроблені для інтеграції з реалізаціями 5G UPF, підтримуючи пропускну здатність перевірки 1 Тбіт/с і вище, щоб задовольнити величезні вимоги до пропускну здатності щільних міських розгортань 5G. DPI в 5G також дозволяє застосовувати політики сегментації мережі, гарантуючи, що критично важливі сегменти, чутливі до затримки, для автономних транспортних засобів або програм дистанційної хірургії отримують абсолютний пріоритет трафіку над сегментами "найкращі зусилля" для споживчого широкосмугового доступу, одночасно контролюючи всі сегменти на наявність аномалій безпеки в режимі реального часу.

3.2 Розробка структурної схеми

Навколо систем глибокого аналізу трафіку сформувався досить міцний ареол міфів, що перешкоджає розумінню функціональних можливостей і рішень для адаптації технології.

DPI як листоноша, що заглядає в конверти

Багато хто стверджують і одночасно побоюються, що системи глибокого аналізу трафіку – це ненадійний листоноша, що вивчає вміст кожної посилки, що доставляється їм. Однак ця аналогія невідповідна. Більше точною аналогією буде листоноша, що розносить вітальні картки або листівки, адже саме на них схожі пакети даних у Мережі – їхній зміст доступно всім.

DPI-системи не використовуються для читання повідомлень, що пересилаються, наприклад по електронній пошті, – вони лише аналізують і встановлюють природу переданого контенту – голос, лист, шкідливе програмне

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32

забезпечення. На підставі отриманих даних вони ухвалюють рішення щодо того, що робити із умістом. Це дозволяє здійснювати захист від DDoS-атак, працювати з рекламою, оптимізувати канали доступу, збирати аналітикові й пріоритизувати трафік. Відзначимо, що всі ці функції реалізує система СКАТ від VAS Experts.

DPI – це порушення приватності

Цей міф є наслідком попереднього. Є думка, що мережний пристрій, що досліджує користувальницький контент, порушує приватність спілкування, як би «прослуховує» дзвінки. Але й це не зовсім так. Впливаючи цій логіці, під визначення «слухача» потраплять і антивіруси, антиспам захист, системи виявлення вторгнень, які важливі для забезпечення безпеки роботи в інтернеті.

Автоматична комп'ютерна система, що сканує файли в пошуках відомих паттернов шкідливого ПЗ або спама, – це не порушення приватності. Насправді, ця процедура менш ретельна, чим огляд багажу в аеропорті. Сканерами управляють люди, що вивчають уміст валіз і сумок і точно ідентифікуючі предмети, що перебувають усередині, у той час як DPI-система реагує лише на запрограмовані сценарії. Виходить, що DPI-рішення в аеропорті «бачило» би в багажі тільки ті предмети, які заборонений проносити на борт літака.

Також хотілося б відзначити, що системи DPI, навпаки, допомагають запобігати випадкам «підслуховування» на лінії. Мова йде про так звані MITM-атаки. Цей термін позначає мережну атаку, коли зловмисник за допомогою спеціального програмного забезпечення підключається між користувачем і додатком, імітуючи роботу з ним і створюючи враження нормального процесу обміну інформацією. Ціль такої атаки може бути сама різна – розкрадання персональних даних користувачів, особистої переписки або банківських реквізитів і ін.

Звичайно MITM-атака проходить у два етапи. Спершу здійснюється перехоплення трафіку, що надходить від користувача до цільового застосунку. Найбільш простим способом перехоплення залишається пасивна атака, коли зловмисник створює відкриті бездротові крапки. У момент підключення

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

користувача до мережі, що атакує одержує доступ до всіх переданим даним. Що стосується інших способів перехоплення -активних – те тут використовуються такі варіанти, як IP-спуфінг, ARP-спуфінг і DNS-спуфінг, що полягають у підміні IP-адреси, MAC-адреси або зараженні DNS відповідно.

Після перехоплення двосторонній SSL-трафік дешифрується, причому так, що користувач і запитуваний їм ресурс не зауважують втручання ззовні. Для цього також існує кілька прийомів: HTTPS-спуфінг, атака SSL Beast, SSL-хайджекинг.

Тому для захисту від MITM-атак розроблювачам веб-застосунків і сайтів варто використовувати захищені протоколи TLS і HTTPS, що ускладнюють проведення спуфінг-атак і перехоплення трафіку. Оператори зв'язку ж використовують системи Deep Packet Inspection для виявлення аномалій у мережах передачі даних і запобігання спуфінга.

DPI виявляться «не при справах» при поширенні шифрування

Є думка, що DPI-рішення почнуть стимулювати адаптацію технологій шифрування, оскільки усе більше користувачів будуть намагатися перешкодити провайдеру «читати» їхню пошту. Однак ріст популярності шифрування буде тільки корисний. Адже реальна погроза споживачам – це доступ до незашифрованих сайтів. У цьому випадку вони стають легкою «видобутком» для зловмисників.

Приміром, Netflix – це найбільша компанія-постачальник відеоконтента у світі. Сервіс має порядку 60 мільйонів передплатників, а на початку 2026 року користувачі «нагляділи» 10 мільярдів годин. Компанія генерує більше третини всього вхідного трафіку на території Північної Америки у вечірній час.

Недавно Netflix заявили, що сервіс почне шифрувати весь переданий трафік, перемінивши протокол передачі даних з HTTP на захищений HTTPS. Таке рішення повинне забезпечити конфіденційність клієнтів і захистити інтелектуальну власність правовласників контенту.

Зараз основна частка зашифрованого трафіку в інтернеті доводиться на Google, Facebook і Twitter. На зображенні нижче вони представляють більшу частину червоного сектора. Після переходу Netflix на HTTPS червоний і зелений сектор поміняються місцями.

З поширенням протоколів шифрування трафіку оператори зв'язку, що використовують системи глибокого аналізу, нібито зіткнулися із проблемою неможливості вивчення даних усередині зашифрованого пакета. Однак представники компаній заявляють, що в них ніколи й не було мети підглядати за діями користувачів.

DPI – це просто інструмент

DPI-технологія досить нейтральна сама по собі. Це просто інструмент, що може бути використаний по-різному. Негативне офарблення DPI-системи придбали через недорозуміння принципів роботи й призначення рішень. Але DPI – це необов'язкове порушення чієїсь приватності або вторгнення в приватне життя, це ще й прискорення роботи мережі, підвищення безпеки й аналіз необхідної статистики.

Використання мобільного широкополосного доступу перебуває на стійкій траєкторії постійного росту, за рахунок росту ринку “розумних” мобільних пристроїв і NG-Інфраструктури, що може обробляти більше даних на більше високих швидкостях. Забезпечення вигідної доставки постійно зростаючих обсягів трафіку з наданням QoS, є важливою й завжди актуальним завданням для операторів, що забезпечує конкурентні переваги.

Створення нових застосунків, що використовують нові можливості, породжує вимога постійного експонентного збільшення пропускної здатності мережної інфраструктури.

Нові підходи й нові можливості в наданні послуг зв'язку:

- залучення незадоволених користувачів інших операторів і провайдерів;
- утримання абонентів серед існуючого числа передплатників;
- збільшення середнього доходу з абонента (ARPU).

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		35

Саме для рішення цих завдань пропонується встаткування, що виконує глибокий пакетний аналіз – Deep Packet Inspection (DPI).

Deep packet inspection (DPI) являє собою технологію мережного моніторингу, що дозволяє операторові зв'язку аналізувати інтернет трафік у режимі реального часу й приймати автоматизовані рішення про подальші дії над ним. Аналіз трафіку за допомогою DPI устаткування дає операторам зв'язку нові можливості, які були недоступні раніше.

Наприклад, DPI дозволяє вирішити питання актуальності модернізації каналів зв'язку, визначити тенденції росту трафіку і його типу, перейти на новий рівень формування сервісних пакетів.

Складно визначити, які саме послуги будуть вимагати користувачі в майбутньому, але ґрунтуючись на поведженні споживачів сьогодні, завтрашні переваги, швидше за все, складуть еkleктичну суміш існуючого набору сервісів, сервісів на основі застосунків і вибіркової їхнього використання (наприклад, послуга батьківський контроль – заборона конкретних сервісів по вимогах окремого користувача). Якщо провайдери будуть готові надавати сервіси нового рівня, тоді й вони і їхні користувачі будуть мати перевагу, від джерела, що має, генерації кастомізованих сервісів. Конкретний набір послуг споживаних клієнтами повинен буде варіюватися з таким же прагненням, з яким буде виникати бажання індивідуалізації сервісів користувачами широкополосного доступу, відповідно до своїх унікальних вимог.

Вибір DPI систем операторського класу:

1. DPI система повинна задовольняти вимоги сьогоdnішньої продуктивності передачі даних (10+ Gbps) і бути масштабованою, при необхідності використання системи з більшою продуктивністю. До того ж, DPI система повинна підтримувати сотні тисяч передплатників і мільйони сесій (IP flows) паралельно, без втрат користува льницького QoS.

2. Важливим у виборі є потужність DPI engine, що забезпечує аналіз мережних застосунків, мережний інтелект і видимість всіх надаваних сервісів.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		36

DPI система, також повинна мати потужний аналізатор сесій у режимі реального часу із заданою продуктивністю, вносячи мінімальні або не вносячи зовсім затримки при аналізі застосунків минаючих по мережі.

3. Відкритість і відповідність стандартам – важливий фактор при виборі DPI системи. Відкрита, стандартизована платформа забезпечує незалежність від запатентованого (proprietary) устаткування й протоколів.

Оператори й постачальники послуг зіштовхуються з нескінченними проблемами відповідності вимогам абонента й появи нових трендів в умовах твердої конкуренції. При цьому, тепер недостатньо просто збільшувати продуктивність каналів і засновувати тарифні плани на більшій пропускній здатності на абонента. Необхідно кардинально міняти підхід до ціноутворення, переходячи на тарифні плани на основі надаваного контенту. Виконувати диференціацію сервісів і тим самим створювати додаткову вартість послуг, користаючись із цієї можливості як джерелом збільшення доходів. Розуміння й контроль, надаваний DPI-системою, дає можливість провайдерам зв'язку персоналізувати сервіси, у результаті чого підвищувати ступінь задоволеності клієнтів (QoS), зменшувати відтік абонентів і підвищувати ARPU (Average revenue per user – середній виторг на один користувача). Вибір DPI-систем повинен бути заснований на їхній відкритості й відповідності галузевим стандартам, перевірених можливостях і реальній продуктивності.

Структурна схема розробленої системи зображена на рисунку 3.1. На ній показано структуру системи, яка складається з наступних блоків:

1. Система виявлення аномалій, яка включає в себе:
 - Модуль взаємодії з базою даних перевірки та фільтрації пакетів.
 - Модуль DPI.
 - Модуль обробки результатів.
 - Інтерфейс адміністратора.
 - Базу даних виборок.
 - Базу даних шаблонів нормального поведження трафіку.

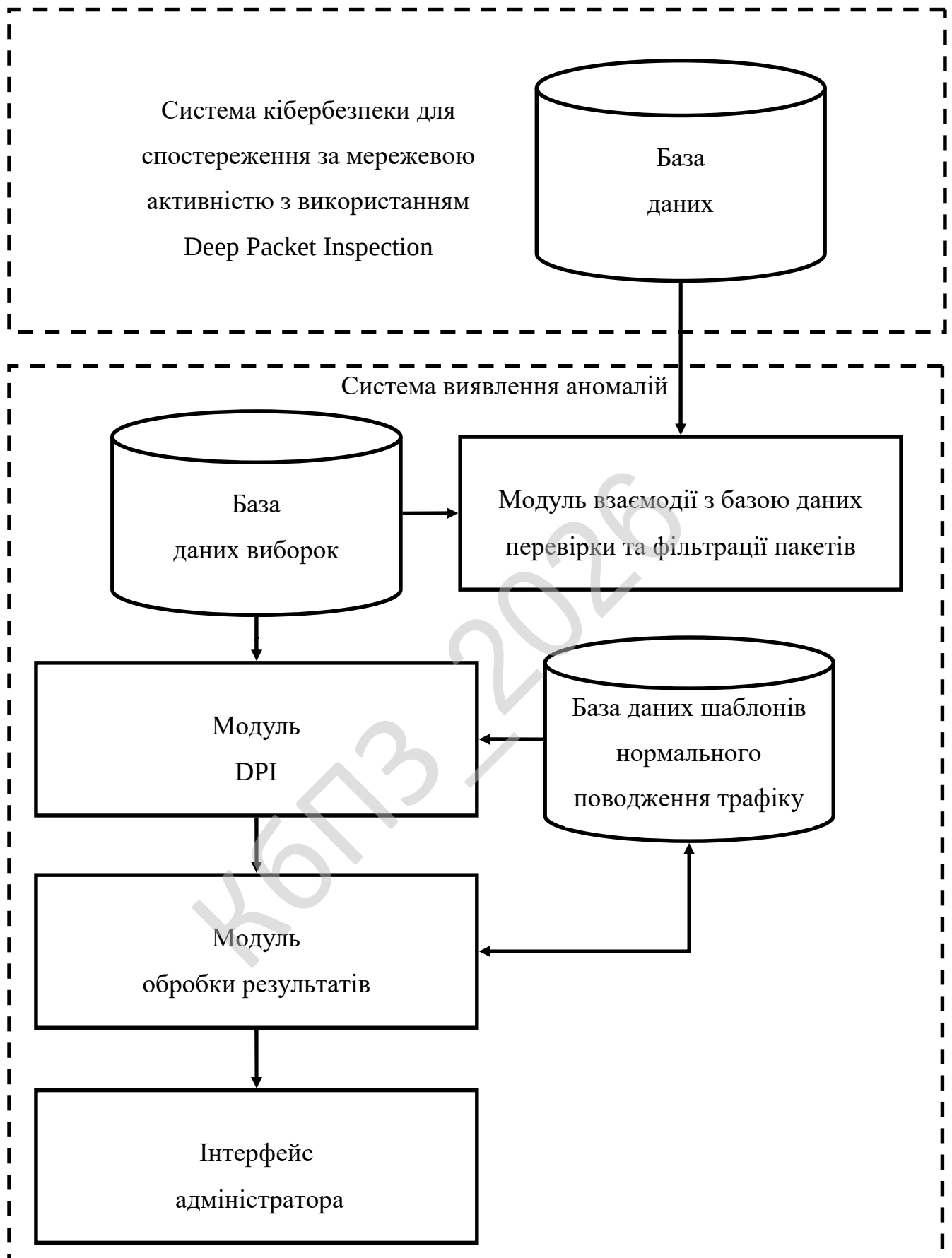


Рисунок 3.1 – Структурна схема системи

2. Система кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection, яка включає в себе Базу даних результатів кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection.

Поява аномалій у різних точках спостереження протягом невеликого проміжку часу говорить про можливий взаємозв'язок подій. Об'єкт, що має більш ранній за часом момент виникнення аномалії може бути джерелом нестандартного поведіння ряду даних. Досліджуючи виникнення аномалій на різних пристроях, можливим є побудова дерева аномалій, що веде від джерела через посередників різних рівнів до приймачів і навпаки: від приймача до джерела.

3.3 Розробка функціональної схеми

Функціональна схема розробленої системи зображена на рисунку 3.2. Так, як функціональна схема є більш подібним описом функціональних можливостей структурної схеми, то вона буде представляти собою, більш детальний варіант структурної схеми.

З рисунку видно, що розроблена система складається з наступних частин:

- Блок визначення топології мережі.
- Блок виявлення аномального поведіння трафіку.
- Блок зберігання результатів.
- Блок визначення виду атаки.
- Блок кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection.

– Блок аналізу мережної статистики.

Блок визначення топології мережі

Блок визначення топології мережі:

- Блок використання відомостей із загальної системи моніторингу мережі, а не опитування пристрою додатково.

- Блок складання списку пристроїв у мережі, автоматично, ґрунтуючись на дані системи моніторингу.
- Блок побудови топології мережі, за станом на задану дату й відстеження змін у топології протягом часу.
- Блок автоматичного визначення рівнів ієрархії пристроїв у мережі, з виділенням периферійних, проміжних і центральних вузлів;
- Блок побудови топології мережі, незалежно від використовуваної системи моніторингу й програмно-апаратних платформ;
- Блок комбінувати показників, на основі яких визначаються зв'язки між пристроями, і при їхньому обчисленні виконувати перевірку на значимість із використанням статистичних критеріїв.

Блок виявлення аномального поведження трафіку

Блок виявлення аномального поведження трафіку:

- Блок визначення профілю поведження нормального трафіку.
- Блок заміни направлення трафіку.
- Блок усунення аномального трафіку.

При первісному розгортанні рішення по DDoS адміністратор створює профіль поведження нормального трафіку. Цей процес іменується навчанням. Компанія використовує додатки звичайним образом протягом 24 годин протягом одного тижня, і трафік застосунку проходить через Детектор аномалій трафіку. У період навчання Детектор аномалій трафіку збирає базову інформацію для розуміння нормальної роботи мережі, куди входять:

- Інтенсивність пакетів для кожного типу пакетів, обмірювана як кількість пакетів у секунду (pps).
- Співвідношення пакетів, наприклад, співвідношення пакетів SYN і пакетів FIN.
- Кількість одночасних ТСР-з'єднань, відкритих одним джерелом.

Базова інформація збирається по кожній цільовій адресі хост-ПК, цільовій підмережі, вихідній адресі хост-ПК і вихідній підмережі.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		40

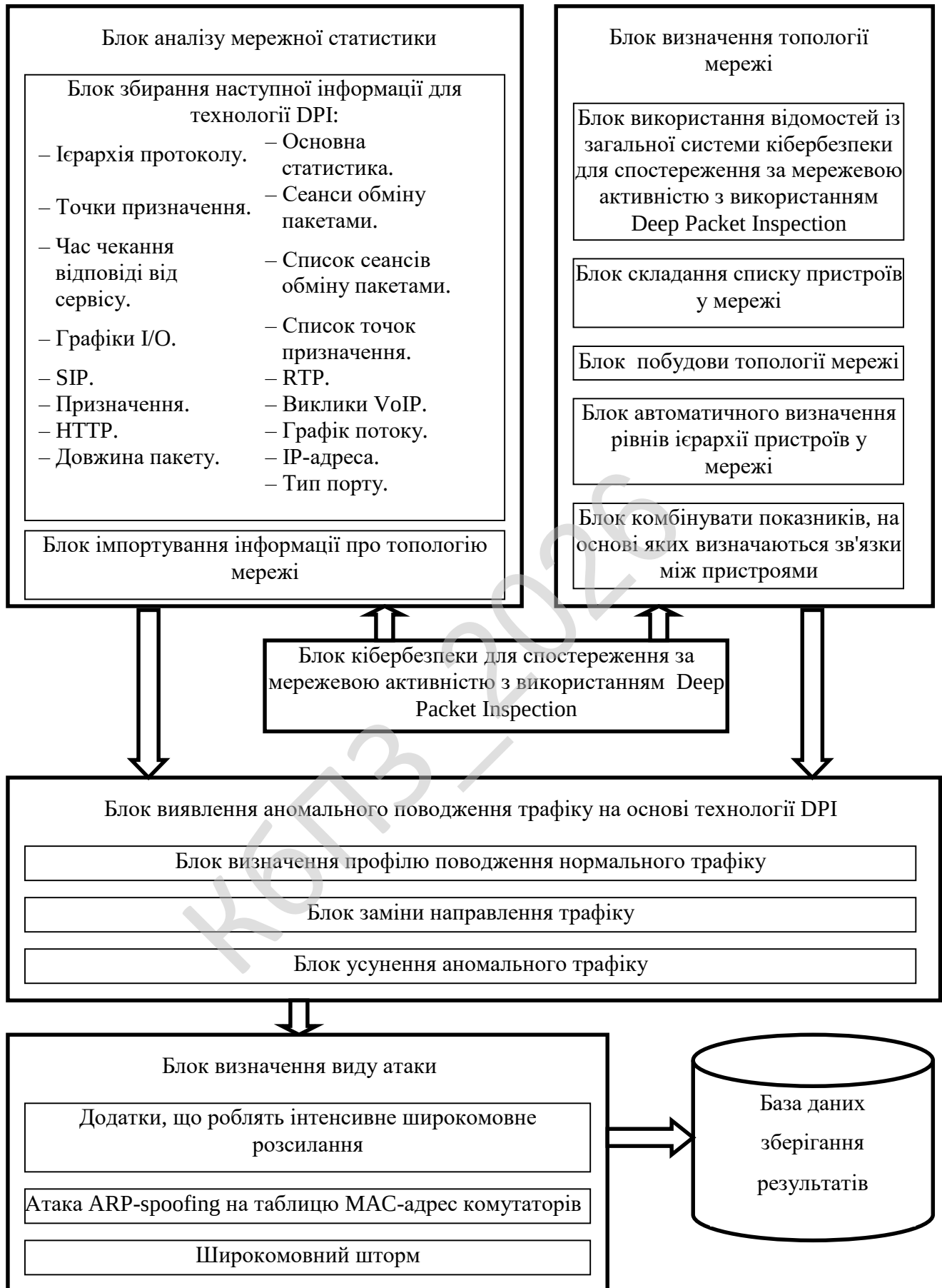


Рисунок 3.2 – Функціональна схема системи

Після закінчення періоду навчання Детектор аномалій трафіку переводиться в режим моніторингу, а Блок усунення аномального трафіку – у резервний режим готовності. Доти, поки немає атаки, що активно розвивається, вхідний трафік з мережі Інтернет проходить через комутатор без якого-небудь втручання з боку Блоку усунення аномального трафіку. Копія вхідного трафіку посилає для аналізу на Детектор аномалій трафіку через зовнішній аналізатор протоколів (SPAN) або віртуальні списки ACL. Якщо Детектор аномалій трафіку виявляє аномальне в порівнянні з базовою інформацією поведження трафіку, починається процес усунення:

- Детектор аномалій трафіку направляє в Блок усунення аномального трафіку команду почати процес зміни напрямку.
- Блок усунення аномального трафіку відхиляє (“захоплює”) трафік, адресований на атакуєму IP-адресу, переадресуючи його на самого себе.
- Блок усунення аномального трафіку піддає трафік багатоступінчастому аналізу й застосовує контрзаходи для відділення благонадійних джерел від джерел атаки. Цей процес іменується очищенням або вичищенням.
- Блок усунення аномального трафіку скидає трафік атаки й пересилає благонадійний трафік назад на нормальний маршрут проходження трафіку до мети. Цей процес іменується ін'єкцією.

Детектор аномалій трафіку

Детектор аномалій трафіку – це пасивний пристрій моніторингу, що постійно виявляє ознаки, що вказують на присутність атаки DDoS, спрямованої проти захищеного місця призначення, також іменованого зоною. Це може бути сервер, інтерфейс міжмережного екрана або інтерфейс маршрутизатора. Детектор аномалій трафіку аналізує копії всього вхідного трафіку, адресуємого в захищені зони, через SPAN або відгалуження пасивної мережі. Цей аналіз включає зіставлення поточного поведження трафіку з базовими граничними параметрами, які також іменуються зональною політикою, для виявлення аномального поведження трафіку. Якщо аномальне поведження виявлене й виглядає як

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		42

можлива атака, Детектор аномалій трафіку через позаполосну управлінську мережу Ethernet посилає в Блок усунення аномального трафіку сигнал про початок аналізу й усунення атаки.

Блок усунення аномального трафіку

Блок усунення аномального трафіку – це автономний пристрій аналізу й фільтрації трафіку. Починаючи прийом трафіку, адресованого в конкретну зону, що, очевидно, піддається атаці, Блок усунення аномального трафіку проводить точний аналіз цього трафіку. Якщо результати аналізу підтверджують, що трафік злочинний, Блок усунення аномального трафіку застосовує контрзаходи, наприклад, механізми анти-спуфінга й фільтрацію різного рівня (таблиця 3.1). Кінцевий результат полягає в тому, що трафік зі злочинних джерел скидається, а трафік із благонадійних джерел пересилається в передбачений пункт призначення.

Атаки DDoS – виявлення й усунення

Перерахуємо типи атак DDoS, які може виявляти й усувати Блок усунення аномального трафіку.

1. Атаки із заповненням смуги пропущення.

Лавинні атаки зі спуфінгом або без спуфінга:

- Прапор TCP (SYN, SYN-ACK, ACK, FIN).
- Протокол керування повідомленнями в Інтернет (ICMP).
- Протокол користувальницьких датаграмм (UDP).

Приклади: лавинна атака SYN, smurf, LAND і UDP – лавинні атаки.

Атаки зомбі-комп'ютерів/мереж зомбі-комп'ютерів, у яких кожний вихідний зомбі-ПК або мережа відкриває множинні TCP-з'єднання й, у деяких випадках, видає багаторазові запити HTTP.

Атаки DNS, наприклад, лавинна атака із запитами DNS.

2. Атаки з дефіцитом ресурсів:

– Атаки пакетного розміру, характерна риса яких – фрагментовані або великі пакети. Приклади: teardrop і ping-of-death.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		43

– Атаки зомбі-комп'ютерів/мереж зомбі-комп'ютерів з низькою інтенсивністю схожі на атаки із заповненням смуги пропускання за тим виключенням, що кожне джерело атаки посилає множинні запити з невеликим обсягом в одиницю часу.

– Атаки DNS з рекурсивним переглядом DNS.

Можливі варіанти зміни напрямку трафіку

Фахівці з ІТ можуть використовувати описані нижче варіанти зміни напрямку трафіку з його пересиланням з мережі, розташованого вище лежачого оператора зв'язку, на Блок усунення аномального трафіку. Цей процес також іменується “захватом” трафіку:

– Повідомлення прикордонного шлюзового протоколу (Border Gateway Protocol, BGP) із Блок усунення аномального трафіку на маршрутизатори, розташовані у вище лежачого оператора зв'язку, з інформацією про те, що трафік, адресований на захищену адресу призначення, буде переспрямований на Блок усунення аномального трафіку.

– Використання зовнішніх механізмів зміни напрямку трафіку, наприклад, маршрутизаторів віддаленого відновлення BGP.

– Повідомлення про ін'єкцію очищеного трафіку на маршруті (Route Health Injection, RHI) від Блок усунення аномального трафіку для процесу маршрутизації в Catalyst серії 6500 або в систему нагляду серії 7600. Ці повідомлення поміщають статичний маршрут у глобальну таблицю маршрутизації, у якій модуль Блок усунення аномального трафіку позначений як наступний вузол.

Можливі варіанти ін'єкції трафіку

Ін'єкція трафіку – це процес, застосовуваний у Блок усунення аномального трафіку для пересилання очищеного благонадійного трафіку в точку призначення, що піддається атаці. Рішення підтримує різні варіанти ін'єкції трафіку. У варіанті 2-ого рівня топології, очищений трафік пересилається із Блок усунення аномального трафіку на статично-конфігуруєму наступну адресу заходу. Ця адреса перебуває на маршрутизаторі, розташованому нижче й

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		44

з'єднанням з тої ж VLAN або підмережею, що й інтерфейс/VLAN ін'єкції трафіку. Ін'єкцію трафіку на 2-му рівні найпростіше конфігурувати, оскільки тут не потрібно вносити які-небудь істотні зміни в конфігурацію маршрутизатора, розташованого нижче.

Варіанти ін'єкції трафіку 3-го рівня:

- Маршрутизація й пересилання по VPN (VPN Routing and Forwarding, VRF).
- Маршрутизація на основі політики (Policy-Based Routing, PBR).
- Транкінг VLAN (VLAN Trunking).
- Інкапсуляція по загальній маршрутизації (GRE) або інкапсуляція IP у тунелі IP (IPIP).

Блок визначення виду атаки

Блок визначення виду атаки:

- Атака ARP-spoofing на таблицю mac-адрес комутаторів.
- Широкомовний шторм.
- Додатки, що роблять інтенсивне ширококомовне розсилання, наприклад: ширококомовні чати й мережні ігри.

ARP-spoofing

ARP-spoofing – техніка атаки в Ethernet мережах, що дозволяє перехоплювати трафік між хостами. Заснована на використанні протоколу ARP.

При використанні в розподіленій обчислювальній системи (PBM) алгоритмів віддаленого пошуку існує можливість здійснення в такій мережі типової віддаленої атаки «помилковий об'єкт PBM». Аналіз безпеки протоколу ARP показує, що, перехопивши на атакуючому хості усередині даного сегмента мережі ширококомовний ARP-запит, можна послати помилкову ARP-відповідь, у якій оголосити себе шуканим хостом (наприклад, маршрутизатором), і надалі активно контролювати мережний трафік дезінформованного хосту, впливаючи на нього за схемою «помилковий об'єкт PBM».

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		45

Протокол ARP призначений для перетворення IP-адрес в MAC-адреси. Найчастіше мова йде про перетворення в адреси Ethernet, але ARP використовується й у мережах інших технологій: Token Ring, FDDI і інших.

Алгоритм роботи ARP

Протокол може використовуватися в наступних випадках:

1. Хост А хоче передати IP-пакет вузлу В, що перебуває з ним в одній мережі.
2. Хост А хоче передати IP-пакет вузлу В, що перебуває з ним у різних мережах, і користується для цього послугами маршрутизатора R.

У кожному із цих випадку вузлом А буде використовуватися протокол ARP, тільки в першому випадку для визначення MAC-адреси вузла В, а в другому – для визначення MAC-адреси маршрутизатора R. В останньому випадку пакет буде переданий маршрутизатору для подальшої ретрансляції.

Далі для простоти розглядається перший випадок, коли інформацією обмінюються вузли, що перебувають безпосередньо в одній мережі. (Випадок коли пакет адресований вузлу, який знаходиться за маршрутизатором, відрізняється тільки тим, що в пакетах переданих після того як ARP-перетворення завершено, використовується IP-адреса одержувача, але MAC-адреса маршрутизатора, а не одержувача.).

Проблеми ARP

Протокол ARP є абсолютно незахищеним. Він не має ніякого способу перевірки дійсності пакетів: як запитів, так і відповідей. Ситуація стає ще більш складною, коли може використовуватися мимовільний ARP (gratuitous ARP).

Мимовільний ARP – таке поводження ARP, коли ARP-відповідь надсилається, коли в цьому (з погляду одержувача) немає особливої необхідності. Мимовільна ARP-відповідь це пакет-відповідь ARP, присланий без запиту. Він застосовується для визначення конфліктів IP-адрес у мережі: як тільки станція одержує адресу по DHCP або адреса привласнюється вручну, розсилається ARP-відповідь gratuitous ARP.

Мимовільний ARP може бути корисний у наступних випадках:

- Відновлення ARP-таблиць, зокрема, у кластерних системах.
- Інформування комутаторів.
- Повідомлення про включення мережного інтерфейсу.

Незважаючи на ефективність мимовільного ARP, він є особливо небезпечним, оскільки з його допомогою можна запевнити віддалений вузол у тому, що MAC-адреса якої-небудь системи, що перебуває з нею в одній мережі, змінилася й указати, яка адреса використовується тепер.

До виконання ARP-spoofing'a в ARP-таблиці вузлів А і В існують записи з IP- і MAC-адресами один одного. Обмін інформацією виробляється безпосередньо між вузлами А і В.

У ході виконання ARP-spoofing'a комп'ютер С, що виконує атаку, відправляє ARP-відповіді (без одержання запитів):

- вузлу А: з IP-адресою вузла В і MAC-адресою вузла С;
- вузлу В: з IP-адресою вузла А і MAC-адресою вузла С.

У силу того що комп'ютери підтримують мимовільний ARP (gratuitous ARP), вони модифікують власні ARP-таблиці й поміщають туди записи, де замість справжніх MAC-адрес комп'ютерів А і В знаходиться MAC-адреса комп'ютера С.

Після того як атака виконана, коли комп'ютер А хоче передати пакет комп'ютеру В, він знаходить в ARP-таблиці запис (він відповідає комп'ютеру С) і визначає з її MAC-адресу одержувача. Відправлений по цьому MAC-адресу пакет приходить комп'ютеру С замість одержувача. Комп'ютер С потім ретранслює пакет тому, кому він дійсно адресований – тобто комп'ютеру В.

Широкомовний шторм

Широкомовний шторм – лавина (сплеск) широкомовних пакетів (на другому рівні моделі OSI – кадрів). Розмноження некоректно сформованих широкомовних повідомлень у кожному вузлі приводить до експонентного росту їхнього числа й паралізує роботу мережі. Звичайно такі пакети використовуються мережними сервісами для оповіщення станцій про свою присутність. Вважається

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		47

нормальним, якщо широкомовні пакети становлять не більше 10% від загального числа пакетів у мережі.

Також досить часто до шторму приводять кільця в мережі при некоректному налаштуванні протоколу Spanning Tree, оскільки в заголовку пакетів Ethernet немає інформації про час життя кадру, як, наприклад, у пакетів IP. Крім цього широкомовний шторм застосовується (навмисно) зломщиками.

Відповідно до галузевого стандарту де-факто число широкомовних і багатоадресних кадрів у мережі не повинне перевищувати 8-10% від загального числа кадрів.

Широкомовний кадр – це кадр, адресований всім станціям у домені мережі. Багатоадресний кадр – це кадр, адресований групі станцій у домені мережі. Оскільки широкомовний кадр адресований всім станціям, то, одержавши його, станції повинні перервати свою роботу й обробити такий кадр. Це сповільнює роботу всієї мережі.

Якщо відношення числа широкомовних кадрів до загального числа кадрів більше 10%, то такий ефект називається "широкомовним штормом".

Широкомовний шторм може бути наслідком дефектів устаткування або неправильного налаштування параметрів активного встаткування. Найчастіше це явище спостерігається в розподілених мережах NetWare, побудованих на основі комутаторів, або коли дані між сегментами або доменами мережі можуть передаватися більш ніж по одному потенційному шляху. Якщо один з комутаторів такої мережі не підтримує протокол Spanning Tree (звичайно IEEE 802.1d) або останній неправильно налаштований або збоїть, то в мережі починається некерована циркуляція широкомовних кадрів.

Виявлення "широкомовного шторму" є не настільки тривіальним завданням, як це може здатися на перший погляд. Для його виявлення недостатньо взяти загальне число широкомовних кадрів і поділити його на загальне число кадрів, що пройшли по мережі.

Для цього ви повинні визначити: яку частку становлять широкомовні кадри в кожний інтервал часу (наприклад, за одну хвилину) і яка при цьому утилізація каналу зв'язку. Якщо, наприклад, за одну хвилину по мережі пройшло 4

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		48

кадри, а 2 з них були широкомовними, то це ще не виходить, що ви спостерігаєте "широкомовний шторм".

Захист від широкомовних штормів (broadcast storm)

Одна з характерних несправностей мережного програмного забезпечення – мимовільна генерація з високою інтенсивністю широкомовних пакетів. Широкомовним штормом вважається ситуація, у якій відсоток широкомовних пакетів перевищує 20% від загальної кількості пакетів у мережі. Звичайний комутатор або міст сліпо передає такі пакети на всі свої порти, як того вимагає його логіка роботи, засмічуючи, таким чином, мережу. Боротьба із широкомовним штормом у мережі, з'єднаної комутаторами, жадає від адміністратора відключення портів, що генерують широкомовні пакети. Маршрутизатор не поширює такі ушкоджені пакети, оскільки в коло його завдань не входить копіювання широкомовних пакетів в усі поєднувані їм мережі. Тому маршрутизатор є прекрасним засобом боротьби із широкомовним штормом, щоправда, якщо мережа розділена на достатню кількість підмереж.

Блок аналізу мережної статистики

Блок збирання наступної інформації:

- Основна статистика (Summary).
- Ієрархія протоколу (Protocol Hierachy).
- Сеанси обміну пакетами (Conversations).
- Точки призначення (Endpoints).
- Графіки I/O (IO Graphs).
- Список сеансів обміну пакетами (Conversation List).
- Список точок призначення (Endpoint List).
- Час чекання відповіді від servісу (Service Response Time).
- RTP.
- SIP.
- Виклики VoIP (VoIP Calls).
- Призначення (Destination).

- Графік потоку (Flow Graph).
- HTTP.
- IP-адреса (IP address).
- Довжина пакету (Packet Length).
- Тип порту (Port Type).

Розпишемо їх більш детально.

1. Основна статистика. Доступні такі елементи основної статистики, як:

- Властивості захоплених файлів.
- Час захвату.
- Інформація про фільтр захвату.
- Інформація про фільтр відображення.

2. Ієрархія протоколу. Статистика ієрархії протоколу допомагає аналізувати пакети, розбиваючи відображені дані, які належать чинному рівню OSI.

3. Сеанси обміну пакетами. Якщо ви використовуєте протокол TCP/IP або програму, яка працює із цим протоколом, ви маєте побачити чотири активних вкладок для обміну пакетами за допомогою Ethernet, IP, TCP та UDP. «Діалог» між комп'ютерами відображає трафік між двома активними хостами. Номер, зазначений на вкладці після назви протоколу, означає кількість «діалогів» між хостами. Номер, зазначений на вкладці після назви протоколу, означає кількість «діалогів» між хостами, наприклад, «Ethernet:6».

4. Точки призначення. Точки призначення забезпечують статистику даними про відправку та прийом пакетів. Номер, зазначений на вкладці після назви протоколу, вказує на кількість точок призначення. Наприклад, «Ethernet:6».

5. Графіки I/O. Основний графік може бути отриманий за допомогою команди «IO graphs» (Графіки I/O). Ще декілька графіків можуть бути додані у тому ж вікні на основі фільтрів відображення.

6. Час чекання відповіді від сервісу. 13 протоколів доступні для глибокого аналізу.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		50

7. RTP. RTP (Real-time Transport Protocol, протокол передачі у реальному часі, RFC 3550) – це протокол для передачі звука та відео через IP-мережу. Він працює у початку протоколу дейтаграм користувача (User Datagram Protocol, UDP). Він часто використовується у сукупності з протоколами SIP або H.233, забезпечуючи виконання сигнальних завдань.

8. SIP. SIP (Session Initiation Protocol, протокол встановлення сесії, RFC 3261) – це сигнальний протокол, який оголошує відео– або VoIP-сесії. Він працює разом із протоколом RTP, який використовується для передачі мультимедійних даних.

9. Виклики VoIP.

VoIP (Voice over IP, голосовий зв'язок за допомогою Інтернету) взагалі використовує два типи протоколів:

- сигнальні протоколи, такі, як SIP або H.323
- переносні протоколи, наприклад, RTP

10 Призначення. Відображення усіх IP-адрес призначення мережевих пакетів.

11. Графік потоків. Графіки потоків забезпечує послідовний аналіз TCP-з'єднань. Перші три строки містять оголошення TCP-з'єднання з послідовностями «SYN», «SYN ACK» та «ACK».

12 HTTP. HTTP (Hypertext Transfer Protocol, протокол передачі гіпертексту) – це протокол типу «клієнт-сервер», який використовується для передачі HTML-файлів. HTTP-клієнт (у більшості випадків це web-браузер) відсилає HTTP-запит до web-серверу із полем «URL», який допомагає знайти потрібний файл. Web-сервер відповідає HTTP-пакетом та забезпечує клієнт необхідною web-сторінкою.

Меню «HTTP» містить три підменю:

- «Load Distribution» (Розподіл пакетів).
- «Packet Counter» (Лічильник пакетів).
- «Requests» (Запити).

14 IP-адреса. Відображення IP-адреси джерела або призначення мережевих пакетів.

15. Довжина пакету.

16. Тип порту. Відображення статистики портів TCP або UDP.

Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

Розглянемо розроблену діаграму процесів яка зображена на рисунку 3.3. Основна будова діаграми процесів полягає у графічному представленні складу сукупностей даних, що характеризуються як співвідношення різних частин кожної з сукупностей. Склад статистичної сукупності графічно може бути представлений як за допомогою абсолютних, так і відносних показників. Графічне зображення складу сукупності по абсолютними і відносними показниками сприяє проведенню більш глибокого аналізу і дозволяє проводити аналіз системи. Діаграма взаємодії процесів використовується для візуалізації процесів обробки даних (структурне проектування). Для розробника вважається звичним спочатку креслити діаграму взаємодії процесів даних рівня контексту, завдяки чому буде показано взаємодію системи. Ця діаграма в подальшому підлягає уточненню шляхом деталізації процесів та потоків даних з метою показати систему що розробляється. При детальному її розгляді можна побачити як саме проходить взаємодія у розробленій системі. Використовується модель проектування, графічне представлення «потоків» даних в інформаційній системі.

Діаграми потоків даних містять чотири типи елементів:

- Зовнішні по відношенню до системи сутності.
- Потоки даних між елементами трьох попередніх типів.
- Процеси які являють собою трансформацію даних в рамках описуваної системи.
- Сховища даних (репозиторії).



Рисунок 3.3 – Діаграма взаємодії процесів

Таким чином, розглянувши опис системи, структурну, функціональну схеми системи, та діаграму взаємодії процесів перейдемо до опису блок-схем основної програми, та підпрограм, які використовуються, для реалізації системи.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Розглянемо реалізацію бакалаврської дипломної роботи. Були проведені розрахунки і підібрані набори тестових даних для перевірки правильності реалізації проектних рішень.

Було створено блок-схеми роботи системи. Перед їх розглядом необхідно провести роз'яснення який саме тип блок-схем використовується. Блок-схема це представлення задачі для її аналізу або розв'язування за допомогою спеціальних символів (геометричних образів), які позначають такі елементи, як операції, потік, дані тощо.

Блок вхідних та вихідних даних прийнято позначати паралелограмом, блок обчислень (обробки) даних – прямокутником, блок прийняття рішень – ромбом, еліпсом – початок та кінець алгоритму.

У інформаційних технологіях функціональна схема складається з функціональних блоків, які являють собою конструктивно відособлені частини (елементи або пристрої) автоматичних систем, які виконують певні функції. Функціональні блоки на схемі позначають прямокутниками, всередині яких надписують їх найменування відповідно до функцій, що виконуються. Зв'язки між функціональними блоками (внутрішні впливи) позначаються лініями зі стрілками, які вказують напрям впливів.

Функціональні схеми можуть виконуватися в укрупненому і розгорненому вигляді. У першому випадку на схемі зображають найважливіші блоки системи і зв'язки між ними.

У другому варіанті схема відображається більш детально, що полегшує її читання та ілюструє принцип роботи.

Основні елементи схем алгоритму це термінатор, процес, рішення, зумовлений процес (підпрограма), дані та з'єднувач. Термінатор це елемент відображає вхід із зовнішнього середовища або вихід з неї (найчастіше застосування – початок і кінець програми). Всередині фігури записується відповідна дія.

Процес це виконання однієї або кількох операцій, обробка даних будь-якого виду (зміна значення даних, форми подання, розташування). Всередині фігури записують безпосередньо самі операції. Рішення це показує рішення або функцію перемикального типу з одним входом і двома або більше альтернативними виходами, з яких тільки один може бути обраний після обчислення умов, визначених всередині цього елемента.

Вхід в елемент позначається лінією, що входить зазвичай у верхню вершину елемента. Якщо виходів два чи три то зазвичай кожен вихід позначається лінією, що виходить з решти вершин (бічних і нижній). Якщо виходів більше трьох, то їх слід показувати однією лінією, що виходить з вершини (частіше нижній) елемента, яка потім розгалужується.

Відповідні результати обчислень можуть записуватися поруч з лініями, що відображають ці шляхи. Зумовлений процес (підпрограма) це символ відображає виконання процесу, що складається з однієї або кількох операцій, що визначені в іншому місці програми (у підпрограмі, модулі). Всередині символу записується назва процесу і передані в нього дані.

Дані це перетворення у форму, придатну для обробки (введення) або відображення результатів обробки (виведення). Цей символ не визначає носія даних (для вказівки типу носія даних використовуються специфічні символи). З'єднувач це символ відображає вихід в частину схеми і вхід з іншої частини цієї схеми.

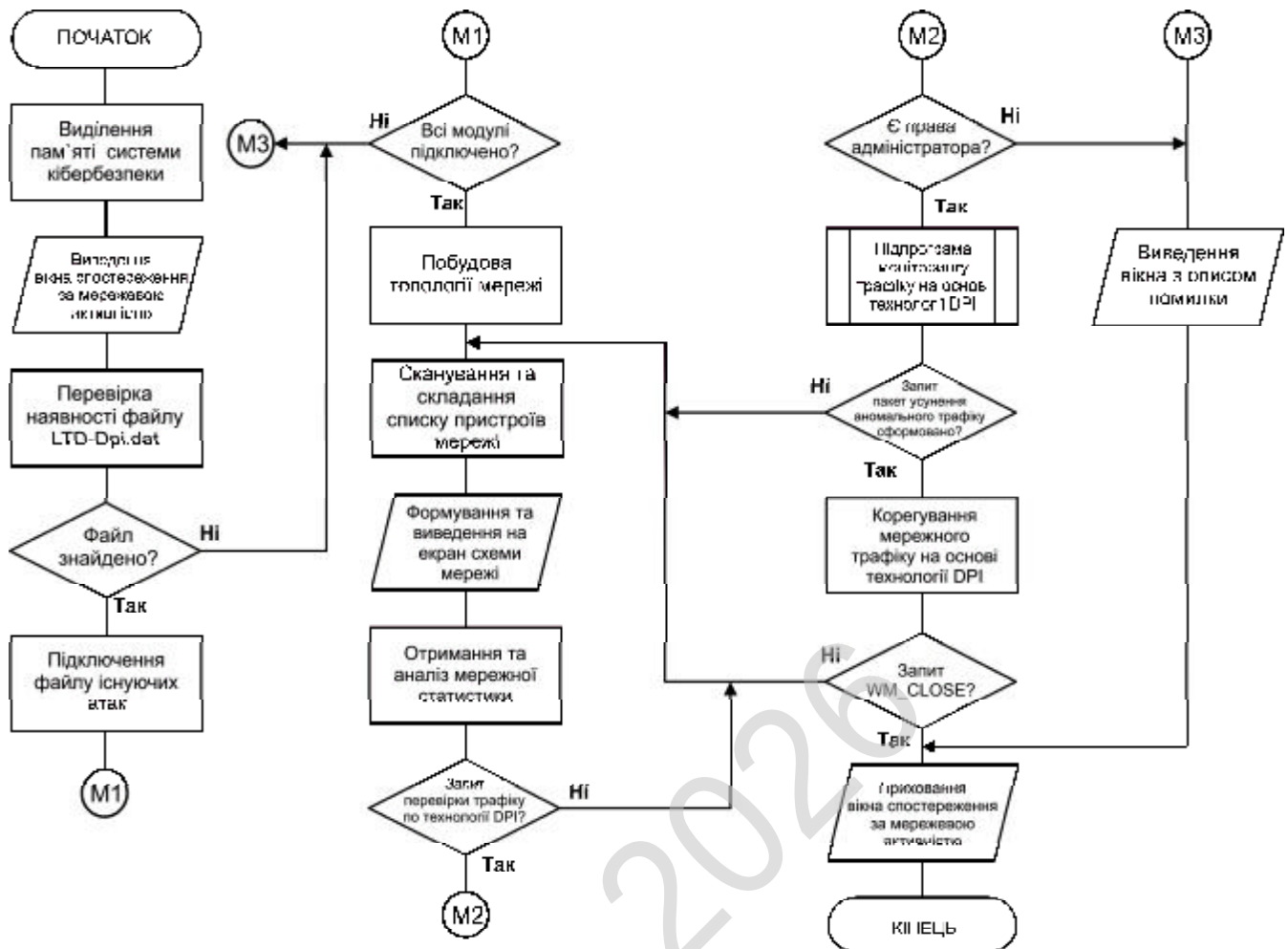


Рисунок 4.1 – Блок-схема основної програми

Використовується для обриву лінії та продовження її в іншому місці (приклад: поділ блок-схеми, що не поміщається на листі). Відповідні сполучні символи повинні мати одне (при тому унікальне) позначення. Блок-схеми показують весь процес роботи системи з підсистемами та частково доказують правильність вибраних проектних рішень. Тому від точності і детальної блок-схеми залежить результат всієї програми. При виборі початкової точки відліку при побудові схем було враховано, що виходячи з вибору мови програмування і інших технічних засобів, програма буде об'єктно-орієнтована що вимагає високого рівня декомпозиції задач на класи.

На рисунку 4.1 зображена основна блок-схема програми, на рисунку 4.2 зображено роботу підпрограми.

З яких видно що робота основної програми складається з початкових етапів ініціалізації ПЗ, перевірки наявності ресурсів системи, блоку початку основного циклу з чеканням запиту від користувача в якому відбувається виклик підсистеми та останньої стадії – перевірка поточного стану з завершенням роботи розробленого ПЗ. При роботі підпрограми виконується основний функціонал системи з циклічними послідовностями, перевіркою поточного стану та поверненням в основну програму прапорів стану виконання.

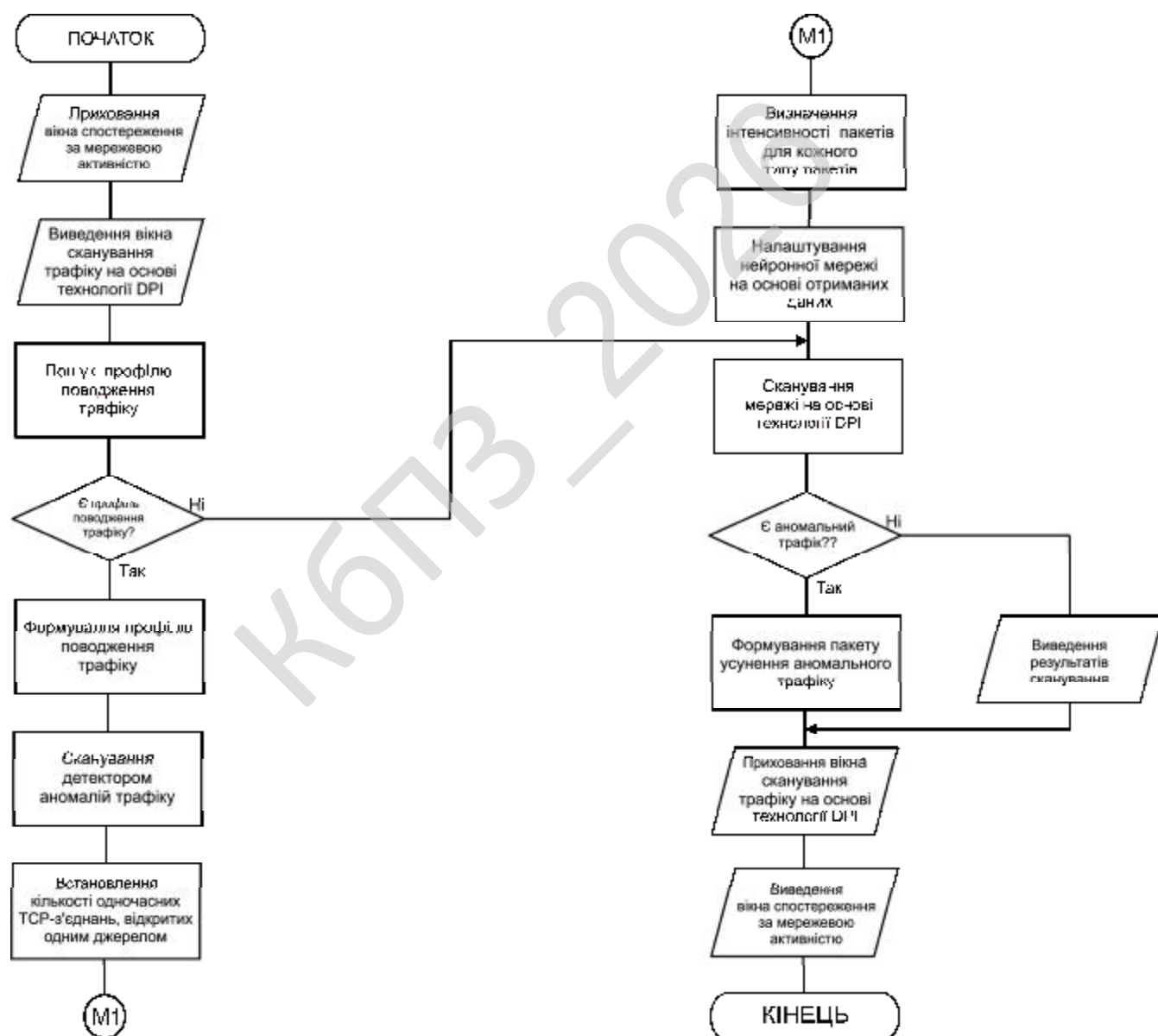


Рисунок 4.2 – Блок-схема роботи підпрограми

Опис архітектури системи

Програмне забезпечення системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection працює як захисний модуль моніторингу комп'ютерної мережі. Система аналізує мережеві пакети, перевіряє заголовки, порти, протоколи, розмір переданих даних та вміст корисного навантаження. Основна мета системи полягає у виявленні підозрілих з'єднань, нетипової активності, заборонених протоколів, ознак витoku даних та потенційних мережевих атак.

Система реалізується мовою Python і використовує модульну архітектуру. Вхідний модуль отримує дані про мережеві пакети. Модуль DPI виконує глибокий аналіз вмісту. Модуль правил порівнює трафік із сигнатурами загроз. Модуль ризику визначає рівень небезпеки. Модуль журналювання зберігає результати перевірки. Модуль звітності формує зведення для адміністратора безпеки.

Основні функції системи

1. Збір інформації про мережеві пакети
2. Аналіз IP адрес, портів, протоколів і напрямку трафіку
3. Перевірка вмісту пакетів за сигнатурами DPI
4. Виявлення підозрілих ключових слів і шаблонів
5. Розрахунок рівня ризику мережевої події
6. Формування повідомлень про інциденти
7. Збереження подій у журналі безпеки
8. Підготовка короткого звіту для адміністратора

Система складається з клієнтського рівня, рівня обробки трафіку, рівня аналізу DPI, рівня збереження даних та рівня звітності. Клієнтський рівень надає адміністратору інформацію про події. Рівень обробки трафіку приймає пакети та виділяє з них основні параметри. Рівень DPI перевіряє корисне навантаження. Рівень збереження фіксує результати перевірки у журналі. Рівень звітності показує кількість безпечних і небезпечних подій.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		58

Розглянемо частину вихідного коду – виклик функції.

```
import re
import sqlite3
from datetime import datetime
class Packet:
    def __init__(self, source_ip, destination_ip, protocol, source_port,
destination_port, payload):
        self.source_ip = source_ip
        self.destination_ip = destination_ip
        self.protocol = protocol
        self.source_port = source_port
        self.destination_port = destination_port
        self.payload = payload

class DPIRule:
    def __init__(self, name, pattern, risk_points):
        self.name = name
        self.pattern = pattern
        self.risk_points = risk_points
    def check(self, payload):
        return re.search(self.pattern, payload, re.IGNORECASE) is not None

class SecurityLog:
    def __init__(self, db_name="dpi_security_log.db"):
        self.connection = sqlite3.connect(db_name)
        self.create_table()
    def create_table(self):
        cursor = self.connection.cursor()
        cursor.execute("""
            CREATE TABLE IF NOT EXISTS events (
                id INTEGER PRIMARY KEY AUTOINCREMENT,
                event_time TEXT,
                source_ip TEXT,
                destination_ip TEXT,
                protocol TEXT,
                destination_port INTEGER,
                risk_level TEXT,
                description TEXT
            )
        """)
        self.connection.commit()
```

```

def save_event(self, packet, risk_level, description):
    cursor = self.connection.cursor()
    cursor.execute("""
        INSERT INTO events (
            event_time,
            source_ip,
            destination_ip,
            protocol,
            destination_port,
            risk_level,
            description
        )
        VALUES (?, ?, ?, ?, ?, ?, ?)
    """, (
        datetime.now().strftime("%Y-%m-%d %H:%M:%S"),
        packet.source_ip,
        packet.destination_ip,
        packet.protocol,
        packet.destination_port,
        risk_level,
        description
    ))
    self.connection.commit()
def close(self):
    self.connection.close()

class DPIAnalyzer:
    def __init__(self):
        self.rules = [
            DPIRule("Підозрілий SQL запит", r"(union select|drop table|or 1=1)", 40),
            DPIRule("Можливий витік пароля", r"(password|passwd|pwd)\s*=", 35),
            DPIRule("Підозрілий командний рядок",
                r"(cmd.exe|powershell|/bin/sh)", 45),
            DPIRule("Передавання токена", r"(api_key|access_token|secret_key)", 30)
        ]
    def analyze_packet(self, packet):
        risk_score = 0
        matched_rules = []
        for rule in self.rules:
            if rule.check(packet.payload):
                risk_score += rule.risk_points
                matched_rules.append(rule.name)

```

```

    if packet.destination_port in [23, 445, 3389]:
        risk_score += 20
        matched_rules.append("Небезпечний або контрольований порт")
    if packet.protocol.upper() not in ["TCP", "UDP", "ICMP"]:
        risk_score += 15
        matched_rules.append("Нетиповий протокол")
    risk_level = self.calculate_risk_level(risk_score)
    if matched_rules:
        description = ", ".join(matched_rules)
    else:
        description = "Ознаки загрози не виявлено"
    return risk_level, description

def calculate_risk_level(self, score):
    if score >= 70:
        return "Критичний"
    if score >= 40:
        return "Високий"
    if score >= 20:
        return "Середній"
    return "Низький"

class NetworkSecuritySystem:
    def __init__(self):
        self.analyzer = DPIAnalyzer()
        self.log = SecurityLog()
    def process_packet(self, packet):
        risk_level, description = self.analyzer.analyze_packet(packet)
        self.log.save_event(packet, risk_level, description)
        return {
            "source": packet.source_ip,
            "destination": packet.destination_ip,
            "protocol": packet.protocol,
            "port": packet.destination_port,
            "risk_level": risk_level,
            "description": description
        }
    def shutdown(self):
        self.log.close()

def main():
    #Демонстраційні пакети імітують вхідний мережевий трафік
    packets = [

```

```

        Packet("192.168.1.10", "192.168.1.20", "TCP", 50500, 80, "GET /index.html
HTTP/1.1"),
        Packet("192.168.1.15", "192.168.1.25", "TCP", 50501, 443,
"password=admin123"),
        Packet("192.168.1.30", "192.168.1.40", "TCP", 50502, 3389, "remote session
request"),
        Packet("192.168.1.50", "192.168.1.60", "TCP", 50503, 8080, "UNION SELECT
username, password FROM users")
    ]
    system = NetworkSecuritySystem()
    for packet in packets:
        result = system.process_packet(packet)
        print("Джерело:", result["source"])
        print("Призначення:", result["destination"])
        print("Протокол:", result["protocol"])
        print("Порт:", result["port"])
        print("Рівень ризику:", result["risk_level"])
        print("Опис:", result["description"])
        print()
    system.shutdown()

```

Архітектура клієнт-сервер є одним із архітектурних шаблонів програмного забезпечення та є домінуючою концепцією у створенні розподілених мережних програм і передбачає взаємодію та обмін даними між ними. Вона передбачає такі основні компоненти:

- набір серверів, які надають інформацію або інші послуги програмам, які звертаються до них;
- набір клієнтів, які використовують сервіси, що надаються серверами;
- мережа, яка забезпечує взаємодію між клієнтами та серверами.

Сервери є незалежними один від одного. Клієнти також функціонують паралельно і незалежно один від одного.

Немає жорсткої прив'язки клієнтів до серверів. Більш ніж типовою є ситуація, коли один сервер одночасно обробляє запити від різних клієнтів; з іншого боку, клієнт може звертатися то до одного сервера, то до іншого. Клієнти мають знати про доступні сервери, але можуть не мати жодного уявлення про існування інших клієнтів.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		62

Дуже важливо ясно уявляти, хто або що розглядається як «клієнт». Можна говорити про клієнтський комп'ютер, з якого відбувається звернення до інших комп'ютерів.

Можна говорити про клієнтське та серверне програмне забезпечення. Нарешті, можна говорити про людей, які бажають за допомогою відповідного програмного та апаратного забезпечення отримати доступ до тієї чи іншої інформації.

Загальноприйнятим є положення, що клієнти та сервери – це перш за все програмні модулі. Найчастіше вони знаходяться на різних комп'ютерах, але бувають ситуації, коли обидві програми – і клієнтська, і серверна, фізично розміщуються на одній машині; в такій ситуації сервер часто називається локальним.

Модель клієнт-серверної взаємодії визначається перш за все розподілом обов'язків між клієнтом та сервером. Логічно можна відокремити три рівні операцій:

- рівень представлення даних, який по суті являє собою інтерфейс користувача і відповідає за представлення даних користувачеві і введення від нього керуючих команд;
- прикладний рівень, який реалізує основну логіку ПЗ і на якому здійснюється необхідна обробка інформації;
- рівень управління даними, який забезпечує зберігання даних та доступ до них.

Дворівнева клієнт-серверна архітектура передбачає взаємодію двох програмних модулів – клієнтського та серверного. В залежності від того, як між ними розподіляються наведені вище функції, розрізняють:

- модель тонкого клієнта, в рамках якої вся логіка ПЗ та управління даними зосереджена на сервері. Клієнтська програма забезпечує тільки функції рівня представлення;

– модель товстого клієнта, в якій сервер тільки керує даними, а обробка інформації та інтерфейс користувача зосереджені на стороні клієнта. Товстими клієнтами часто також називають пристрої з обмеженою потужністю: кишенькові комп'ютери, мобільні телефони та ін.

Типовим прикладом клієнт-серверної взаємодії є WWW. Існує величезна кількість веб-серверів, на яких розміщується та чи інша інформація. У найпростішому випадку ця інформація являє собою набір веб-сторінок, які можуть зберігатися на сервері у вигляді файлів, розмічених за допомогою мови розмітки HTML. Але ситуація, як правило, є складнішою; значна частина веб-ресурсів на сучасному етапі є динамічними, тобто вони не існують в заздалегідь підготовленому вигляді, а створюються безпосередньо в процесі обробки запиту від користувача.

Для того, щоб людина, яка працює в Інтернеті, могла переглянути ту чи іншу сторінку, на її комп'ютері повинно бути встановлено відповідне програмне забезпечення. Програми для перегляду веб-сторінок називаються браузером.

Але, крім браузерів, до серверів можуть звертатися і інші клієнти, а саме – автономні програми. Вони можуть передбачати взаємодію з людиною, а можуть працювати в цілком автоматичному режимі. Типовим класом таких програм є роботи, призначені для автоматичного перегляду веб-ресурсів. Зокрема, роботи є важливим елементом пошукових систем і використовуються ними для перегляду сторінок і збору інформації про них.

Для запиту до веб-сервера клієнтська програма повинна задати місцезнаходження комп'ютера, на якому розміщується серверна програма, назву потрібного документа і, можливо, інші дані, які специфікують запит. Мережа забезпечує знаходження сервера і передачу йому клієнтського запиту. Серверні програми обробляють цей запит, відповідь пересилається по мережі клієнтові.

Трирівнева клієнт-серверна архітектура, яка почала розвиватися з середини 90-х років, передбачає відділення прикладного рівня від управління даними. Відокремлюється окремий програмний рівень, на якому зосереджується

прикладна логіка ПЗ. Програми проміжного рівня можуть функціонувати під управлінням спеціальних серверів ПЗ, але запуск таких програм може здійснюватися і під управлінням звичайного веб-сервера. Нарешті, управління даними здійснюється сервером даних.

Для роботи з системою користувач використовує стандартне програмне забезпечення – звичайний браузер. Це позбавляє його необхідності завантажувати та інсталиувати спеціальні програми (хоча інколи така необхідність все-таки виникає).

Але користувачеві слід надати в розпорядженні інтерфейс, який дозволяв би йому взаємодіяти з системою і формувати запити до неї. Форми, що визначають цей інтерфейс, розміщуються на веб-сторінках та завантажуються разом з ними.

Веб-оглядач формує запит та пересилає його до сервера, який здійснює обробку. При необхідності сервер викликає серверні програмні модулі, які забезпечують обробку запиту і в разі потреби звертаються до сервера даних. Сервер даних здійснює операції з даними, що зберігаються в системі та складають її інформаційну основу. Зокрема, він може здійснити вибірку з інформаційної бази відповідно до запиту та передати її модулю проміжного рівня для подальшої обробки. Дані, з якими працює сервер даних, найчастіше організовані як реляційна база даних.

Найчастіше веб-сервер і серверні модулі проміжного рівня розміщуються на одному комп'ютері, хоч і являють собою окремі і логічно незалежні програмні модулі.

На сучасному етапі для програмування модулів проміжного рівня використовується мова серверних сценаріїв PHP, а для управління даними – СУБД MySQL. Таким чином, зв'язку PHP-MySQL слід розглядати як стандартний інструмент для створення порівняно простих інтерактивних веб-сайтів та систем електронної комерції; близько 90% комерційних систем сьогодні створюється саме на цій основі. Водночас як засоби управління даними, так і middleware-

засоби можуть бути найрізноманітнішими. Так, для створення серверних програм, крім PHP, широко застосовуються Java, Perl, Python, Delphi.

Взагалі, технології створення розподілених, зокрема веб-програм, стрімко розвиваються. Слід згадати про технології EJB (Enterprise Java Beans), CORBA, а також про .NET – порівняно нову ініціативу компанії Microsoft. Для зберігання даних та їх передачі часто використовується так звана розширювана мова розмітки XML (Extensible Markup Language).

Redmine – вільне серверне ПЗ для управління проектами та відстежування помилок. До системи входить календар-планувальник та діаграми Ганта для візуального представлення ходу робіт за проектом та строків виконання. Redmine написано на мові Ruby і є ПЗ розробленим з використанням відомого веб-фреймворку Ruby on Rails, що означає легкість в розгортанні системи та її адаптації під конкретні вимоги. Для кожного проекту можна вести свої вікі та форуми.

Функціональні можливості:

- Ведення декількох проектів.
- Гнучка система доступу з використанням ролей.
- Система відстеження помилок.
- Діаграми Ганта та календар.
- Ведення новин проекту, документів та управління файлами.
- Сповіщення про зміни за допомогою RSS-потоків та електронної пошти.
- Власна Wiki для кожного проекту.
- Форуми для кожного проекту.
- Облік часових витрат.
- Налаштування власних (custom) полів для задач, затрат часу, проектів та користувачів.
- Легка інтеграція із системами керування версіями (SVN, CVS, Git, Mercurial, Bazaar и Darcs).
- Створення записів про помилки на основі отриманих листів

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		66

- Підтримка LDAP автентифікації.
- Можливість самореєстрації нових користувачів.
- Багатомовний інтерфейс (у тому числі українська мова).
- Підтримка СКБД: MySQL, PostgreSQL, SQLite.

Діаграма Ганта (Gantt chart, також стрічкова діаграма, графік Ганта) – це популярний тип діаграм, який використовується для ілюстрації плану, графіка робіт за будь-яким проектом. Є одним з методів планування та управління проектами.

Діаграма Ганта являє собою відрізки (графічні плашки), розміщені на горизонтальній шкалі часу. Кожен відрізок відповідає окремому завданню або підзадачі. Завдання і підзадачі, складові плану, розміщуються по вертикалі. Початок, кінець і довжина відрізка на шкалі часу відповідають початку, кінцю і тривалості завдання. На деяких діаграмах Ганта також показується залежність між завданнями.

Діаграма може використовуватися для представлення поточного стану виконання робіт: частина прямокутника, що відповідає завданню, заштриховується, відзначаючи відсоток виконання завдання. показується вертикальна лінія, що відповідає моменту «сьогодні».

Часто діаграма Ганта використовується спільно з таблицею зі списком робіт, рядки якої відповідають окремо взятій задачі, зображеній на діаграмі, а стовпці містять додаткову інформацію про задачу.

Система відстеження помилок Багтрекер – прикладна програма для допомоги розробникам програмного забезпечення (програмістам, тестувальникам тощо) враховувати і контролювати помилки, знайдені у програмах, питання щодо функціональності, рішення та оновлення, побажання користувачів, а також стежити за процесом їх виконання.

Кожному, хто розробляв програмні продукти, добре знайоме співвідношення «20/80» – останні 20 % роботи тривають 80 % часу. Як це не парадоксально, але нічого дивного в цій пропорції немає, адже саме на

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		67

завершальній стадії починається тестування проекту, коли виявляються помилки, і що більший проект, то більше буде знайдено помилок. Водночас досить часто виявляється, що більшість цих помилок були відомі та могли бути виправлені з меншими витратами на попередніх стадіях роботи, але не були вчасно описані, а потім загубилися серед інших важливих завдань.

Отже, система відстеження помилок у найпростішому варіанті – це процес, що включає в себе виявлення помилки, її опис, виправлення і перевірку цього виправлення, тобто процес «стеження» за багом протягом всього як його життєвого циклу, так і життєвого циклу розробки в цілому.

Сукупність інформації про дефект. Головний компонент такої системи – база даних, що містить відомості про виявлені дефекти. Ці відомості можуть включати в себе:

- номер (ідентифікатор) дефекту;
- хто повідомив про дефект;
- дата і час виявлення дефекту;
- версія продукту, в якій виявлено дефект;
- серйозність (критичність) дефекту та пріоритет рішення;
- опис кроків для відтворення дефекту (неправильної поведінки програми);
- відповідальний за усунення дефекту;
- обговорення можливих рішень та їх наслідків;
- поточний стан виправлення дефекту;
- версії продукту, в якій дефект виправлений.

Крім того, розвинені системи надають можливість прикріплювати файли, які допомагають описати проблему, наприклад, дамп пам'яті або скріншот.

Використання. Основна перевага систем відстеження помилок полягає в забезпеченні чітких централізованих оглядів, запитів на розробку (включаючи помилки і виправлення) та їх стан. У корпоративному середовищі, системи відстеження помилок можуть бути використані для генерації звітів по продуктивності програмістів виправлення помилок. Однак, це може іноді

приводити до неточних результатів, тому що різні помилки можуть мати різні ступені пріоритету та серйозності, що пов'язано з складністю їх фіксації.

Життєвий цикл дефекту. Як правило, система відстеження помилок використовує той чи інший варіант «життєвого циклу» помилки, стадія якого визначається поточним станом помилки.

Типовий життєвий цикл дефекту:

1. Новий – дефект зареєстрований тестувальником.
2. Призначений – призначений відповідальний за виправлення дефекту.
3. Дозволений – дефект переходить назад у сферу відповідальності тестувальника. Як правило, супроводжується резолюцією, наприклад:

- Виправлено (виправлення включені у версію таку-то).
- Дубль (повторює дефект, що вже знаходиться в роботі).
- Не виправлено (працює відповідно до специфікації, має занадто низький пріоритет, виправлення відкладено до наступної версії тощо).
- «В мене все працює» (запит додаткової інформації про умови, в яких дефект проявляється).

4. Далі тестувальник проводить перевірку виправлення, залежно від чого дефект або знову переходить у стан «Призначений» (якщо він описаний як виправлений, але не виправлений), або у стан «Закрито».

5. Відкрито повторно – дефект знайдено знову в іншій версії.

Система може надавати адміністраторові можливість налаштування користувачі, які можуть переглядати і редагувати помилки залежно від їх стану, переводити їх в інший стан або видаляти.

У корпоративному середовищі, система відстеження помилок може використовуватися для отримання звітів, що показують продуктивність програмістів при виправленні помилок. Однак, часто такий підхід не дає достатньо точних результатів через те, що різні помилки мають різну ступінь серйозності та складності. При цьому серйозність проблеми прямо не стосується складності її усунення.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		69

4.2 Захист розробленого програмного забезпечення

Для захисту розробленого програмного забезпечення запропоновано використовувати алгоритм Khufu. Khufu – це 64-бітовий блоковий шифр. 64-бітовий відкритий тест спочатку розщеплюється на дві 32-бітові половини, L і R . Над обома половинами й певними частинами ключа виконується операція XOR. Потім, аналогічно DES, результати проходять деяку послідовність раундів. У кожному раунді молодший значущий байт L використовується як вхід S-блоку. У кожного S-блоку 8 вхідних біт і 32 вихідних біта. Далі обраний в S-блоці 32-бітовий елемент піддається операції XOR з R . Потім L циклічно зрушується на число, кратним восьми біткам, L і R міняються місцями, і раунд завершується. Сам S-блок не статичний, він міняється кожні вісім раундів. Нарешті, по закінченні останнього раунду, над L і R виконується операція XOR з іншими частинами ключа, і половини поєднуються, утворюючи блок шифртексту.

Хоча частини ключа використовуються для операції XOR із блоком шифрування на початку й кінці виконання алгоритму, головне призначення ключа – генерація S-блоків. Ці S-блоки секретні, по суті, це частина ключа. Повний розмір ключа алгоритму Khufu дорівнює 512 біт (64 байт), алгоритм надає спосіб генерації S-блоків по ключу.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1 зображено розроблене у бакалаврської дипломної роботі система кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи:

- Функціональних кнопок ПЗ.
- Верхнього меню: Файл; Deep Packet Inspection; Налаштування; Довідка.
- Розділу обрання групи.
- Розділу виведення результату роботи системи.



Рисунок 5.1 – Головне вікно ПЗ

Розроблена програма має дуже простий і зрозумілий інтерфейс з користувачем. Кожен, хто в достатньому обсязі володіє операційним середовищем Windows без особливих складностей освоїть і цю програму, оскільки її інтерфейс інтуїтивно зрозумілий. Якщо програма не видала ніяких помилок, і працює, то можна використовувати, інакше слід слідувати інструкціям, які пропонує програма.

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

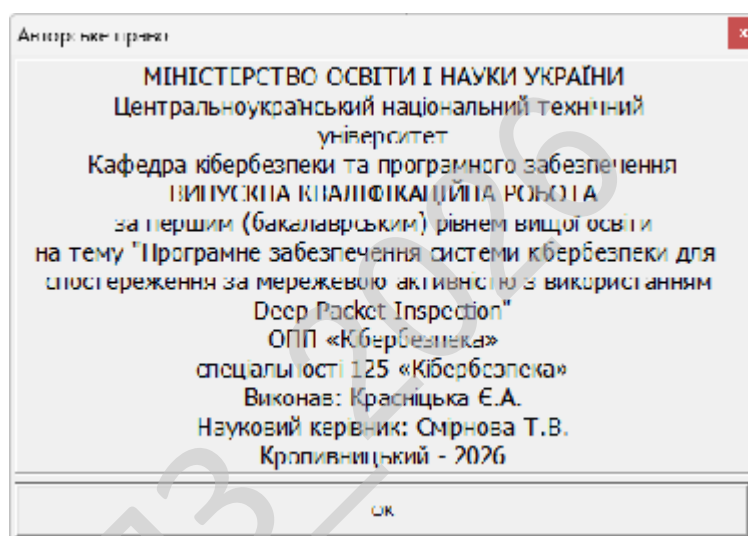


Рисунок 5.2 – Авторське право

Розглянемо процес впровадження програмного забезпечення, це процес налаштування програмного забезпечення під певні умови використання, а також навчання користувачів роботі з програмним продуктом. Впровадження програмного забезпечення це усі дії, що роблять розроблену програмну систему готовою до використання. Даний процес є частинною життєвого циклу програмного забезпечення.

Загалом процес розгортання складається з кількох взаємопов'язаних дій із можливими переходами між ними. Ця активність може відбуватися як з боку виробника так і з боку споживача. Оскільки кожна програмна система є

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		72

унікальною, то усі процеси та процедури під час розгортання важко передбачити. Тому, "розгортання" можна трактувати як загальний процес відповідно до певних вимог та характеристик. Розгортання може здійснюватись програмістом і в процесі розробки програмного забезпечення.

До діяльностей пов'язаних із розгортанням програмного забезпечення відносять:

- Випуск.
- Встановлення та активація.
- Деактивація.
- Адаптація.
- Оновлення.
- Вмонтування.
- Відстежування версій.
- Видалення.
- Вилучення з обігу.

При впровадженні програмного забезпечення потрібно урахувати наступні дії:

– Виділення критичних, з точки зору загального результату, процедур в діяльності організації. Коли набір таких процедур визначений, необхідно в першу чергу використовувати ІТ рішення для автоматизації операцій усередині саме цих процедур. Таким чином, розроблене ІТ рішення автоматично стає життєво важливим і затребуваним для організації, а також буде забезпечена публічність процесу впровадження;

– Розширення нормативної бази організації шляхом включення до неї регламентів, що описують порядок виконання процедур автоматизованих процесів. В іншому випадку є небезпека виникнення неузгодженості між автоматизованими процедурами та іншими процесами організації.

– Виконання робіт з загальної стандартизації існуючої діяльності організації, коли виділяються кращі практики виконання процедур і включаються

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		73

в ІТ рішення за принципом найбільшої корисності для більшості учасників. Відсоток таких процедур щодо загального обсягу автоматизації може бути невеликий, але це надає процесу побудови рішення вагу в організації за рахунок збільшення його необхідності.

Під час роботи над програмою було проведено тестування програмного забезпечення, тобто технічне дослідження, призначене для виявлення інформації про якість продукту відносно контексту, в якому воно має використовуватись.

Тестування включає як процес пошуку помилок або інших дефектів, так і випробування програмних складових з метою їх оцінки.

Проводилась оцінка:

- відповідності поставленим вимогам;
- правильна відповідь для усіх можливих вхідних даних;
- виконання функцій за прийнятний час;
- практичність;
- сумісність з ОС та стороннім ПЗ.

Оскільки число можливих тестів для програмних компонент практично нескінченне, тому стратегія тестування полягала в тому, щоб провести всі можливі тести з урахуванням наявного часу та ресурсів.

Як результат ПЗ тестувалось стандартним виконанням програми з метою виявлення помилок або інших дефектів.

Проводилось тестування форматом білої скриньки засноване на аналізі керуючої структури програми. Програма вважається повністю перевіреною, якщо проведено вичерпне тестування маршрутів (шляхів) її графа управління.

У цьому випадку формуються тестові варіанти, в яких:

- Гарантується перевірка всіх незалежних маршрутів програми.
- Знаходяться гілки True, False для всіх логічних рішень.
- Виконуються всі цикли (у межах їхніх кордонів та діапазонів).
- Аналізується правильність внутрішніх структур даних.

Недоліки тестування "білої скриньки":

- Кількість незалежних маршрутів може бути дуже велика.
- Повне тестування маршрутів не гарантує відповідності програми вихідним вимогам до неї.

- У програмі можуть бути пропущені деякі маршрути.

- Не можна виявити помилки, поява яких залежить від даних.

Переваги тестування "білої скриньки" пов'язані з тим, що принцип «білої скриньки» дозволяє врахувати особливості програмних помилок:

- Кількість помилок мінімально в «центрі» і максимально на «периферії» програми.

- Попередні припущення про ймовірність потоку керування або даних у програмі часто бувають некоректними. У результаті типовим може стати маршрут, модель обчислень за яким опрацьована слабо.

- При записі алгоритму програмного забезпечення у вигляді тексту на мові програмування можливе внесення типових помилок трансляції (синтаксичних та семантичних).

- Деякі результати в програмі залежать не від вихідних даних, а від внутрішніх станів програми.

Проводилось тестування чорної скриньки.

Основне місце програми тестів «чорної скриньки» – інтерфейс ПЗ. Відомі: функції програми. Досліджується: робота кожної функції на всій області визначення.

Ці тести демонструють:

- Як виконуються функції програми.

- Як приймаються вихідні дані.

- Як виробляються результати.

- Як зберігається цілісність зовнішньої інформації.

При тестуванні «чорної скриньки» розглядаються системні характеристики програм, ігнорується їхня внутрішня логічна структура. Вичерпне тестування, як правило, неможливе.

Наприклад, якщо в програмі 10 вхідних величин і кожна приймає по 10 значень, то кількість тестових варіантів становитиме 10^{10} . Тестування «чорної скриньки» не реагує на багато особливостей програмних помилок.

Тестування «чорної скриньки» (функціональне тестування) дозволяє отримати комбінації вхідних даних, які забезпечують повну перевірку всіх функціональних вимог до програми.

Програмний виріб тут розглядається як «чорна скринька», чію поведінку можна визначити тільки дослідженням його входів та відповідних виходів. При такому підході бажано мати:

- Набір, утворений такими вхідними даними, які призводять до аномалій у поведінці програми (назвемо його ІТс).

- Набір, утворений такими вхідними даними, які демонструють дефекти програми (назвемо його ОТ).

Будь-який спосіб тестування «чорної скриньки» повинен:

- Виявити такі вхідні дані, які з високою ймовірністю належать набору ІТс;
- Сформулювати такі очікувані результати, які з високою ймовірністю є елементами набору ОТ.

Принцип «чорної скриньки» не альтернативний принципу «білої скриньки». Скоріше це доповнює підхід, який виявляє інший клас помилок.

Тестування «чорної скриньки» забезпечує пошук наступних категорій помилок:

- Некоректних чи відсутніх функцій.
- Помилки інтерфейсу.
- Помилки у зовнішніх структурах даних або в доступі до зовнішньої бази даних.
- Помилки характеристик (необхідна ємність пам'яті і т.д.).

– Помилки ініціалізації та завершення.

Обрано умови розповсюдження – Shareware. Під умовно-безплатним програмним забезпеченням можна розуміти спосіб або метод розповсюдження комерційного ПЗ на ринку (тобто на шляху до кінцевого користувача), при якому випробувачеві пропонується обмежена за можливостями (не повнофункціональна або демонстраційна версія), терміном дії (тріал версія) або версія з вбудованим набридливим нагадуванням про необхідність оплати використання програми.

В угоді про використання (ліцензії для кінцевого користувача, EULA) також може бути обумовлена заборона на комерційне або професійне (не тестове) її використання.

Основний принцип умовно-безплатного ПЗ – «спробуй, перш ніж купити» (try before you buy). ПЗ що поширюється як умовно-безплатний, надається користувачам безоплатно. Звичайно користувач платить тільки за час завантаження файлів через Інтернет або за носій (CD диск, флешку, ключ). Протягом певного терміну, що становить зазвичай тридцять днів, він може користуватися програмою, тестувати її, освоювати її можливості.

Якщо після закінчення цього терміну користувач вирішить продовжити використання ПЗ, він зобов'язаний купити його (zareєструватися), заплативши авторові певну суму.

В іншому випадку користувач повинен припинити використання ПЗ та видалити його зі свого комп'ютера.

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем для спостереження за мережевою активністю з використанням Deep Packet Inspection.
- Досліджена система для спостереження за мережевою активністю з використанням Deep Packet Inspection.
- На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання для спостереження за мережевою активністю з використанням Deep Packet Inspection.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створенні програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня Python. Дана мова програмування дозволяє найбільш ефективно обробляти дані призначені для

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		78

системи кібербезпеки для спостереження за мережевою активністю з використанням Deep Packet Inspection. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи кібербезпеки й включає програми, що реалізують її функції.

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10/11.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм Khufu.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		79

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Massimo Bertaccini. Cryptography Algorithms. Packt Publishing. 2022. 358 p.
2. Alyssa Miller. Cybersecurity Career Guide. Manning Publications. 2022. 368 p.
3. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBOK The Cyber Security Body of Knowledge. The National Cyber Security Centre. 2019. 854 p.
4. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 p.
5. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.
6. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.
7. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.
8. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p
9. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.
10. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.
11. Kuznetsov O., Frontoni E., Arnesano M., Smirnov O., Khruskov B. «Biometric Authentication in TinyML: Opportunities and Challenges». *Tiny Machine Learning: Design Principles and Applications*, 2026, pp. 587-633.
12. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61.

13. Chulinda L., Smirnov O., Shapenko L., Ustynova I., Bohatiuk I., Kelyp S. «The role of innovation in ensuring the safety of international civil aviation». *Ceur Workshop Proceedings*, 2025, 4024, pp. 530–542.

14. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А, Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.

15. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704–716, 2025

16. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.

17. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.

18. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.

19. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with

Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.

20. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241.

21. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.

22. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447.

23. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. № 2(26), С. 170–188.

24. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.

25. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.

26. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем ІР-телефонії». *Підводні технології*, 2024, № 13, с. 28-35.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		82

27. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.

28. Akhalaia, G., Iavich, M., Iashvili, G., Prysiashnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings*, 2023, 3550, pp. 313-320.

29. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56

30. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchov, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.

31. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings*, Volume 3504, 2023, pp. 1-11.

32. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppapapati, C., Beligiannis, G.N. (eds) *Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.

33. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». *Кібербезпека: освіта, наука, техніка*, №3(19), 2023, С. 176-196.

34. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». *II Міжнародна науково-практична Інтернет-конференція «Інновації та*

перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2023))» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.

35. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.

36. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.

37. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.

38. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings*, Volume 3187, 2022,

39. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». *Journal of Ambient Intelligence and Humanized Computing* Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.

40. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління*, № 2(70). 2022. С. 28-37.

41. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 3(69). С. 93-98.

42. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»*, № 2 (307). С. 46-52. 2022.

43. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.

44. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». *11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021*, Cracow, Poland, 22-25 September 2021. P. 414-418

45. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». *4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021*, Lviv, Ukraine, September 21-25, 2021. P. 255-260.

46. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». *2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020*, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.

					ВКРБ-125.26.0035.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		85

47. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». *CEUR Workshop Proceedings* Volume 2805, 2020, Pages 44-58.

48. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.

49. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.

50. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.

51. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 122-131.

52. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 1-14.

53. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». *Lecture Notes in Networks and Systems*, vol 152. Springer, Cham. 2021, pp 66-84.

54. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 161-165.