УДК 621.391
DOI https://doi.org/10.32782/2663-5941/2024.3.2/02

Бешлей Г.В.
Національний університет «Львівська політехніка»

Іванюк М.М.
Національний університет «Львівська політехніка»

Бешлей М.І.
Національний університет «Львівська політехніка»

РОЗРОБКА ПРОТОТИПУ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ДЛЯ ТЕСТУВАННЯ ТА РОЗВИТКУ СИСТЕМ МОНІТОРИНГУ ZABBIX

У роботі представлено прототип мережевої інфраструктури, розроблений для дослідження та вдосконалення систем моніторингу, зокрема Zabbix. Прототип, розроблений як тестовий майданчик, що забезпечує безпечне середовище для проведення експериментів, мінімізуючи ризики для реальної інфраструктури. Актуальність дослідження обумовлена необхідністю швидкого та ефективного реагування на аномалії та загрози в телекомунікаційних мережах із використанням моніторингових систем .

Прототип мережевої інфраструктури включає мережеве обладнання, таке як роутери, комутатори та сервери, інтегровані з системою моніторингу Zabbix. Налаштовано віртуальну машину з розширеним обсягом оперативної пам'яті та мережевим з'єднанням у режимі моста, що забезпечує стабільне середовище для проведення тестувань. Встановлено систему моніторингу Zabbix з автоматизованою процедурою додавання нових хостів, що значно спрощує управління мережею та інтеграцію нових пристроїв. Інтеграція чат-бота Telegram у систему моніторингу дозволила автоматично надсилати адміністраторам повідомлення про інциденти, підвищуючи оперативність реагування на проблеми. Для аналізу стійкості системи до DDoS-атак створено скрипт на мові програмування C, який протестовано у середовищі Termux. Проведене тестування продемонструвало здатність системи виявляти та реагувати на різноманітні види атак, а також виявило слабкі місця у захисті. Модернізація тригерів для виявлення аномалій у мережі підвищила ефективність реагування на загрози та дозволила вчасно виявляти проблеми. Такий підхід дає можливість ідентифікувати та усувати потенційні загрози на ранніх етапах, що є важливим для забезпечення надійності та безпеки телекомунікаційних систем.

Майбутня робота передбачає подальше вдосконалення системи моніторингу із використанням алгоритмів машинного навчання для аналітики та прийняття рішень, розширення функціональних можливостей чат-бота та автоматизованих процедур, а також проведення додаткових тестувань для підвищення надійності та безпеки телекомунікаційних мереж. Планується дослідження впливу різних типів кіберзагроз та розробка нових методів їх виявлення та нейтралізації.

Ключові слова: *система моніторингу, прототип телекомунікаційної мережі, симуляція DDoS-атаки, тригери, виявлення аномалій, надійність, реагування на загрози.*

Постановка проблеми. Сучасні телекомунікаційні мережі стають дедалі складнішими та інтегрованішими, забезпечуючи критично важливі функції для широкого спектра користувачів і підприємств. З ростом кількості підключених пристроїв та обсягів переданих даних, мережі стають більш вразливими до різних видів аномалій і кібератак, що може значно призводити до зниження якості обслуговування, перебоїв у роботі, витоку конфіденційних даних та інших негативних наслідків [1]. Захист та забезпечення стабільної роботи таких мереж потребує надійних інструментів для моніторингу, виявлення та реагування на різноманітні аномалії та атаки. Моніторинг програмного та апаратного забезпечення телекомунікаційної мережі відіграє ключову роль, надаючи системним адміністраторам можливість оперативно реагувати на аномалії для забезпечення стабільної роботи системи. Основним завданням моніторингу є своєчасне оповіщення про помилки в програмній або апаратній частині системи. Чим швидше здійснюється оповіщення, тим краще для організації, оскільки це дозволяє оперативно усунути причину виникнення помилки і уникнути

можливих витрат [2]. Проте тестування нових методів та удосконалення систем моніторингу у реальних мережах може бути небезпечним, спричиняючи збої у роботі мережі або втрати, які впливають на користувачів і бізнес-процеси.

Аналіз останніх досліджень і публікацій. Аналіз останніх наукових досліджень та публікацій в галузі системи моніторингу Zabbix свідчить про неперевершений прогрес у цій сфері. Від вивчення новітніх технологій до вдосконалення методів аналізу даних, наукові групи та експерти постійно вдосконалюють платформу Zabbix, забезпечуючи її перевагу над конкурентами [3].

Один з основних напрямків досліджень – це застосування машинного навчання та штучного інтелекту для покращення функціональності Zabbix. Впровадження новітніх алгоритмів аналізу даних дозволяє ефективно виявляти аномалії та передбачати можливі проблеми, що забезпечує безперебійну роботу інфраструктури та запобігає можливим витратам через збої [1]. Крім того, значну увагу приділяють питанням кібербезпеки та захисту даних у системі Zabbix. Запровадження передових методів шифрування, аутентифікації та авторизації забезпечує високий рівень захищеності і надійності для інформації, що зберігається та обробляється системою. Значна частина досліджень також спрямована на підвищення інтеграційних можливостей Zabbix з іншими системами та платформами. Це відкриває нові можливості для комплексного моніторингу та управління, забезпечуючи користувачам більш широкий спектр інструментів для вирішення їх потреб [4].

У підсумку, дослідження та розробки в галузі системи моніторингу Zabbix демонструють постійний розвиток та інновації, що робить цю платформу необхідним інструментом для будь-якої компанії, яка прагне забезпечити стабільність та ефективність своєї інфраструктури [5].

Постановка завдання. Саме тому, метою роботи є розробка прототипу телекомунікаційної мережі, яка дозволяє тестувати удосконалені системи моніторингу та досліджувати вплив аномалій на поведінку мережі й якість обслуговування, є вкрай важливою.

Наше дослідження спрямоване на вирішення кількох критичних проблем:

- Забезпечення безпечного тестування нових методів моніторингу без ризику для реальних мереж.
- Виявлення та аналіз впливу аномалій на телекомунікаційну мережу.
- Підвищення ефективності виявлення та реагування на проблеми.
- Зменшення ризиків для користувачів і бізнес-процесів шляхом оптимізації систем моніторингу.

Виклад основного матеріалу. У даній роботі розроблено прототип телекомунікаційної мережі, що дозволяє досліджувати вплив аномалій на поведінку мережі та якість обслуговування. Це рішення забезпечує безпечне тестування нових методів моніторингу, виключаючи ризики, пов'язані з використанням реальних мереж. Прототип складається з роутера (маршрутизатора), комутаторів рівня L2 (D-Link DES-3526), декількох персональних комп'ютерів та телефону із встановленим терміналом Termux, на якому буде створюватись скрипт для DDoS-атак для перевірки відмовостійкості сервера. Переваги цього підходу включають: безпечне тестування, що дозволяє уникнути можливих збоїв та втрат; детальний аналіз впливу аномалій на мережу та якість обслуговування, що сприяє вдосконаленню систем моніторингу; автоматизація процесів додавання нових хостів до моніторингу, що значно полегшує управління мережевими ресурсами; гнучкість та масштабованість, яка робить прототип універсальним інструментом для різноманітних дослідницьких задач; покращення якості обслуговування завдяки швидкому виявленню та реагуванню на проблеми, що підвищує загальну ефективність мережевої інфраструктури. Таким чином, розроблений прототип є важливим інструментом для подальших досліджень та вдосконалення систем моніторингу, забезпечуючи надійний і безпечний спосіб тестування в умовах, максимально наближених до реальних. Структурну схему локальної мережі пристроїв показано на рис. 1.

Прототип телекомунікаційної мережі пристроїв показано на рис. 2.

Розгорнуто систему моніторингу Zabbix на персональному комп'ютері та імпортовано віртуальну машину для подальшого тестування. Налаштовано віртуальну машину, збільшено обсяг оперативної пам'яті до 4096 Мб і встановлено мережеве з'єднання в режимі моста. Після завантаження віртуального сервера використано логін і пароль за замовчуванням для отримання доступу до сервера, отримано IP-адресу сервера і перевірено його доступність у локальній мережі.

Для забезпечення зручності та безпеки здійснено вхід на сервер за допомогою SSH через термінал PuTTy, змінено часовий пояс PHP у файлі zabbix.conf, перезавантажено служби PHP-FPM, надано серверу статичну IP-адресу і вимкнено DHCP-клієнт на інтерфейсі.

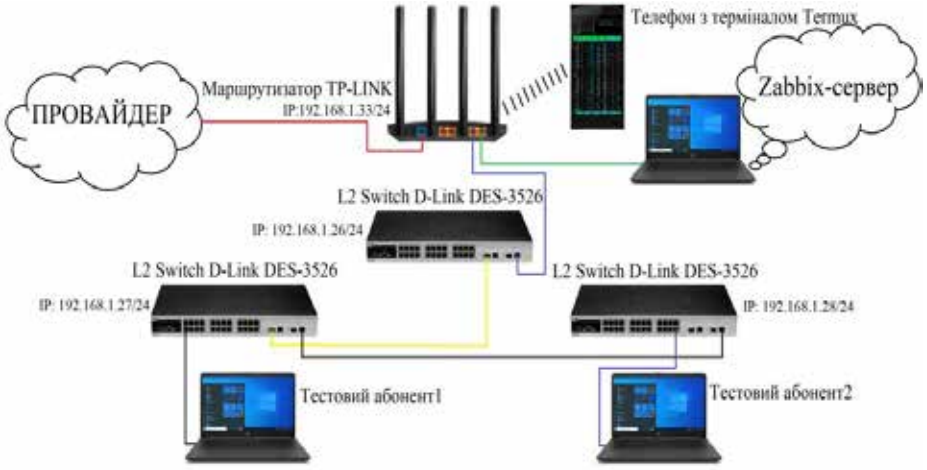

Рис. 1. Структурна схема прототипу локальної мережі

Рис. 2. Прототип телекомунікаційної мереж

Здійснено вхід у веб-інтерфейс Zabbix за статичною IP-адресою сервера, налаштовано систему моніторингу для відстеження стану пристроїв, мережевого трафіку, використання процесора, виконання процесів та інших параметрів

Для автоматизації процесів впроваджено автоматичне додавання хостів, що значно спрощує управління мережевими ресурсами. Система автоматично виявляє нові хости в діапазоні IP: 192.168.1.1/24 та додає їх до моніторингу, підвищуючи ефективність і зменшуючи витрати часу на управління.

Для цього вибрано назву групи для наших моніторингових пристроїв і пулу IP-адрес, які потрібно відслідковувати. Період оновлення встановлюємо 1 хвилину. На рис. 3. показано встановлення параметрів у веб-інтерфейсі Zabbix.

В Discovery check вибрано протокол SNMPv2, 161 порт (tcp/udp), SNMP OID 1.3.6.1.2.1.1.1.0, 1.3.6.1.2.1.1.5.0, а також SNMP community – public. Процес встановлення параметрів для автоматичного моніторингу хостів показано на рис. 4. OID 1.3.6.1.2.1.1.1.0 використовується для отримання значення sysDescr, що представляє опис системи (наприклад, назва, версія, виробник тощо) у мережевому пристрої через SNMP, а OID 1.3.6.1.2.1.1.5.0 використовується для отримання значення sysName, що представляє назву системи (наприклад, ім'я хоста) у мережевому пристрої через SNMP [6].

Кінцевий вигляд сконфігурованої системи автоматичного додавання хостів в Zabbix-сервері показаний на рис. 5.

На комутаційному обладнанні, яке підлягає моніторингу, обрано SNMP community – public для забезпечення взаємодії між системою моніторингу Zabbix та мережевими пристроями. Скріншот налаштування SNMP community на комутаційному обладнанні наведено на рис. 6. Використання цього SNMP дозволяє отримувати доступ до даних про стан мережі без необхідності складних налаштувань або авторизації на кожному пристрої.

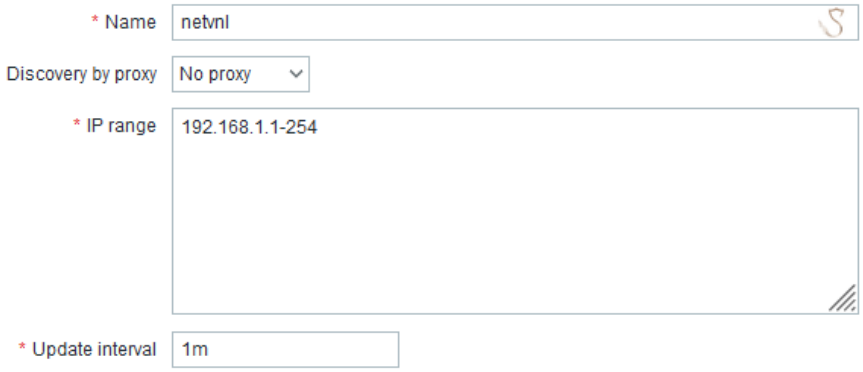

Рис. 3. Встановлення параметрів у веб-інтерфейсі Zabbix

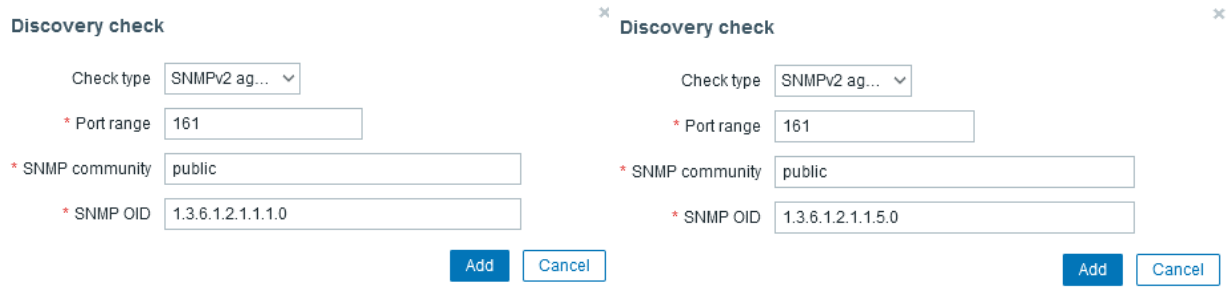

Рис. 4. Встановлення параметрів для моніторингу хостів

Рис. 5. Кінцевий вигляд системи автоматичного додавання хостів

```
DBS-3526:admin#show snmp community
Command: show snmp community

SNMP Community Table
Index : private
Community Name                  View Name                       Access Right
------------------------------  ------------------------------  ------------
private                         CommunityView                   read_write
Index : public
Community Name                  View Name                       Access Right
------------------------------  ------------------------------  ------------
public                          CommunityView                   read_only

Total Entries : 2

DES-3526:admin#
```

Рис. 6. Скріншот встановлення SNMP community на комутаційному обладнанні

Після декількох хвилин очікування, система автоматично виявила хости шляхом сканування мережі та ідентифікації активних пристроїв, провела аналіз їх параметрів, таких як доступність, використання ресурсів та статус з'єднання, і додала їх до моніторингу для подальшого контролю та аналізу. На рис. 7 показано результат автоматичного додавання хостів.

Для того, щоб система відображала реакцію на атаку, необхідно розробити чат-бот в Telegram для сповіщень й інтегрувати його в систему моніторингу. Процес створення чат-бота та отримання токена доступу відображено на рис. 8.

Отримавши токен доступу, інтегруємо чат-бота в систему моніторингу Zabbix. На рис. 9 показано процес інтеграції чат-бота в систему моніторингу Zabbix.

Name ▲	Interface	Availability
Router1	192.168.1.33: 161	ZBX SNMP JMX IPMI
Switch1	192.168.1.28: 161	ZBX SNMP JMX IPMI
Switch2	192.168.1.27: 161	ZBX SNMP JMX IPMI
Switch3	192.168.1.26: 161	ZBX SNMP JMX IPMI
Zabbix server	127.0.0.1: 10050	ZBX SNMP JMX IPMI

Рис. 7. Результат автоматичного додавання хостів

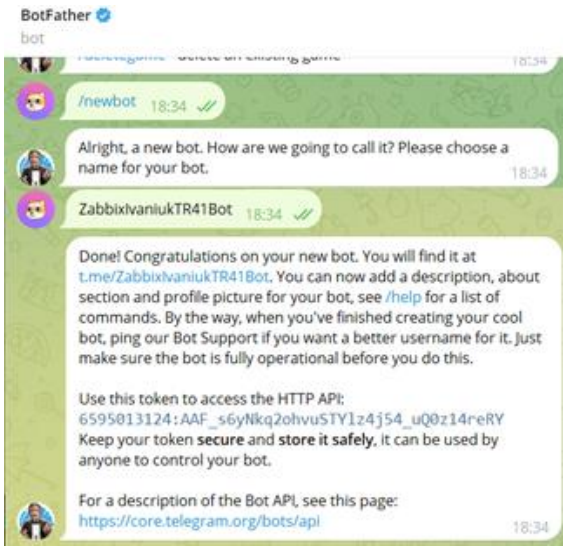

Рис. 8. Створення чат-боту та отримання токена доступу

Рис. 9. Інтеграція чат-бота в систему моніторингу Zabbix

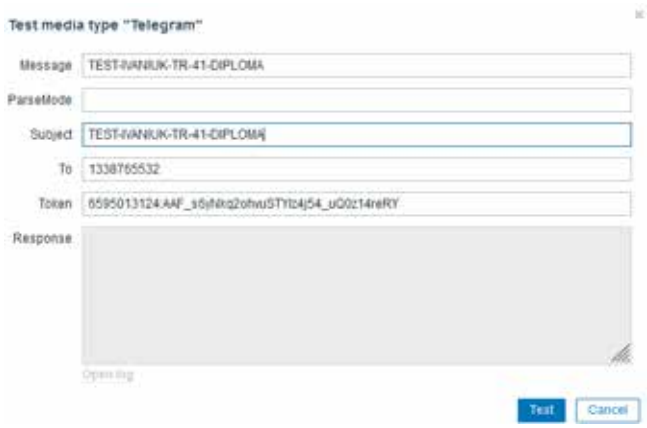

Рис. 10. Створення тестового повідомлення для перевірки коректної роботи

Проведемо перевірку чат-бота, відправивши тестове повідомлення з Zabbix-сервера (рис. 10).

Результат перевірки чат-боту показаний на рис. 11.

Рис. 11. Результат перевірки коректної роботи чат-бота й системи моніторингу

В результаті попередніх кроків ми успішно створили чат-бота та інтегрували його в систему моніторингу Zabbix. З цим кроком завершено, тепер ми можемо перейти до наступних етапу, а саме створення скрипта на мові програмування C, який використовуватиметься для DDoS-атак. Написаний скрипт для DDoS-атак показано на рис. 12.

Процес компіляції DDoS-атаки показано на рис. 17.

Як результат, система сповістила про надмірне навантаження центрального процесора через критичні навантаження під час DDoS-атаки, а чат-бот у Telegram відразу проінформував про цю проблему (рис. 14).

Наведемо декілька графіків з діючої системи моніторингу після закінчення DDoS-атаки, можна ствердити, що усі показники сервера зросли до максимального значення: Сервер отримує над-

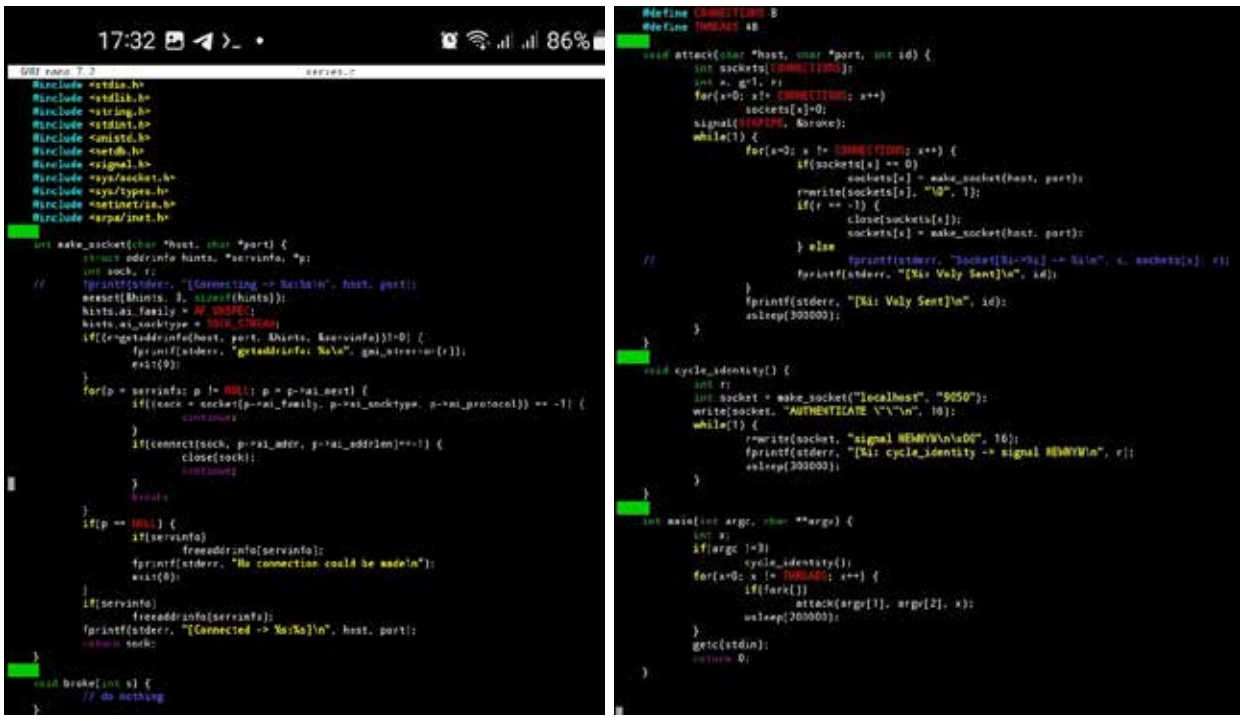

Рис. 12. Написаний скрипт у середовищі Termux на мові програмування С

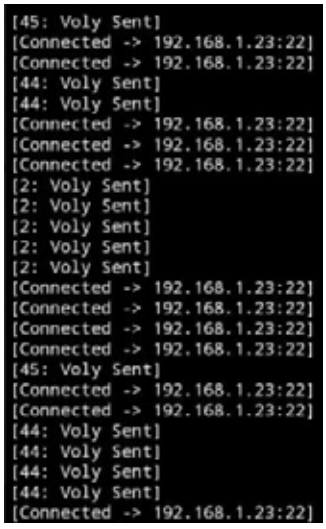

Рис. 13. Запуск скрипта для здійснення DDoS-атаки на сервер

мірний обсяг запитів з великої кількості джерел. Коли це відбувається, сервер витрачає ресурси на обробку кожного запиту або пакету даних. Якщо ця кількість запитів перевищує можливості сервера, то це призводить до перевантаження його обчислювальних можливостей, включаючи центральний процесор, що відображено на рис. 15 та рис. 16. Це призводить до деградації швидкості обробки запитів, збільшення часу відгуку сервера, що відображено на рис. 17 та рис. 18. Задля того, щоб краще зрозуміти вплив DDoS-атаки, сформуємо графіки доступності сервера до моменту проведення й під час проведення, які відображені на рис. 19 та рис. 20.

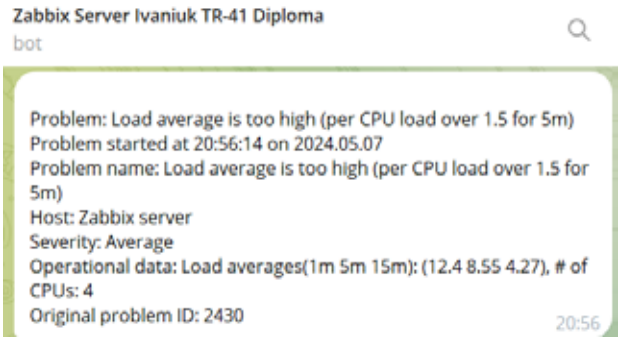

Рис. 14. Реакція чат-бота в телеграмі на аномальний трафік

Як наслідок, атака призвела до деградації швидкості обробки запитів, збільшення часу відгуку сервера. Сервер знаходиться в межах локальної мережі, відповідно його працездатність напряму пов'язана з її станом. Під час DDoS-атаки надходить велика кількість запитів, весь цей потік даних проходить через мережу до сервера. Це означає, що маршрутизатори, комутатори та інші мережеві пристрої також є перенавантаженими обробкою додаткового трафіку. В даному випадку це призвело до зниження швидкості мережі інтернету, що відображено на рис. 21, і збільшення часу відгуку для всіх пристроїв у мережі, що відображено на рис. 22.

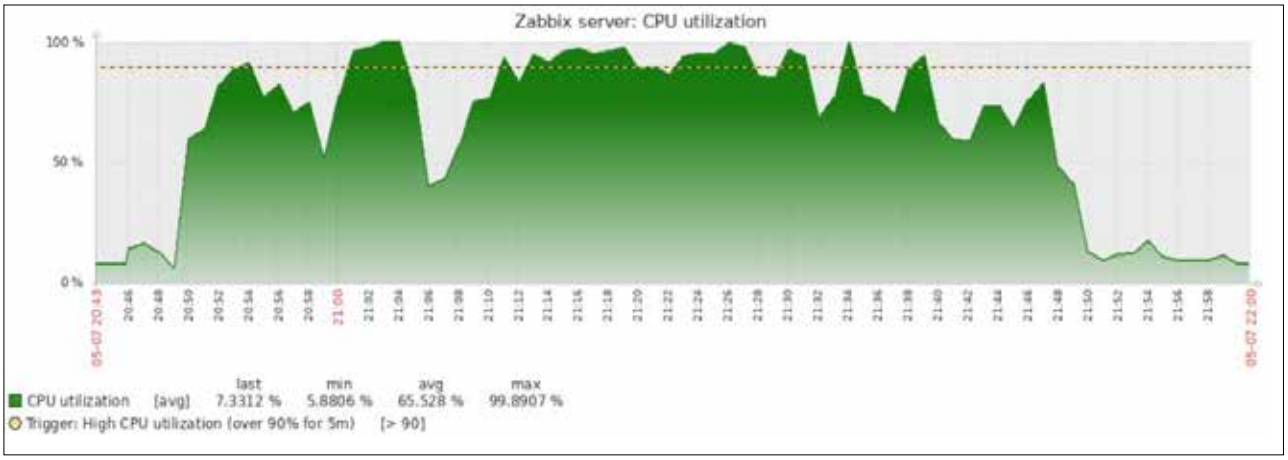

Рис. 15. Графічне відображення навантаженості центрального процесора сервера, під час проведення DDoS-атаки

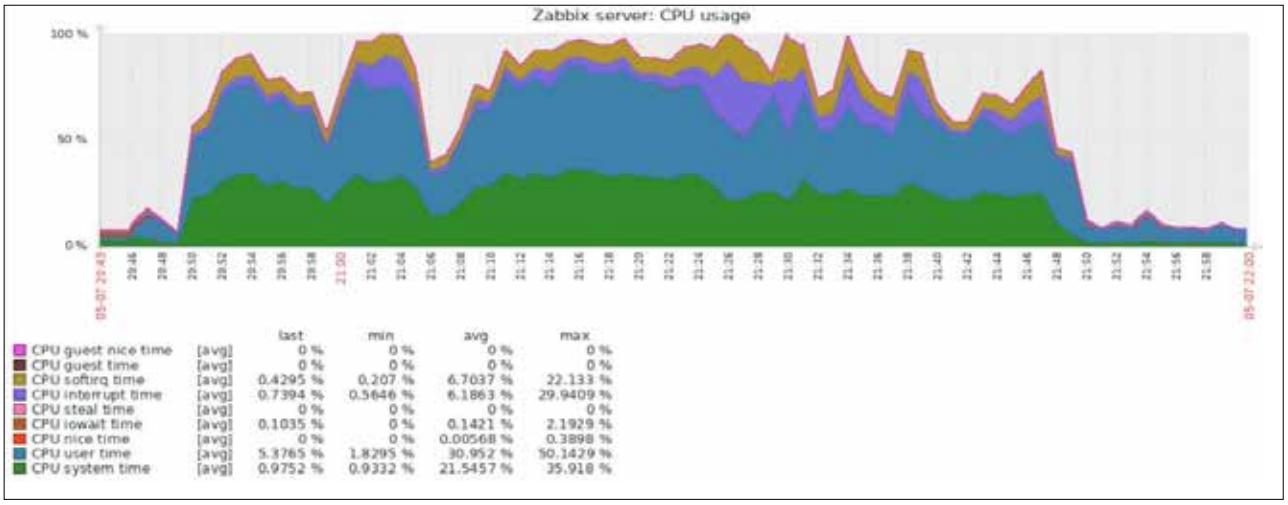

Рис. 16. Графічне відображення використання ресурсу центрального процесора сервера, під час проведення DDoS-атаки

```
C:\Users\Admin>ping 192.168.1.23 -t

Pinging 192.168.1.23 with 32 bytes of data:
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
Reply from 192.168.1.23: bytes=32 time=1ms TTL=64
Reply from 192.168.1.23: bytes=32 time=1ms TTL=64
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
Reply from 192.168.1.23: bytes=32 time<1ms TTL=64
```

Рис. 17. Перевірка доступності серверу до проведення DDoS-атаки

```
C:\Users\Admin>ping 192.168.1.23 -t

Pinging 192.168.1.23 with 32 bytes of data:
Reply from 192.168.1.23: bytes=32 time=134ms TTL=64
Reply from 192.168.1.23: bytes=32 time=436ms TTL=64
Reply from 192.168.1.23: bytes=32 time=9ms TTL=64
Reply from 192.168.1.23: bytes=32 time=109ms TTL=64
Reply from 192.168.1.23: bytes=32 time=1ms TTL=64
Reply from 192.168.1.23: bytes=32 time=664ms TTL=64
Reply from 192.168.1.23: bytes=32 time=340ms TTL=64
Reply from 192.168.1.23: bytes=32 time=19ms TTL=64
Reply from 192.168.1.23: bytes=32 time=546ms TTL=64
Reply from 192.168.1.23: bytes=32 time=24ms TTL=64
Reply from 192.168.1.23: bytes=32 time=39ms TTL=64
Reply from 192.168.1.23: bytes=32 time=15ms TTL=64
Reply from 192.168.1.23: bytes=32 time=178ms TTL=64
Reply from 192.168.1.23: bytes=32 time=20ms TTL=64
```

Рис. 18. Перевірка доступності серверу під час проведення DDoS-атаки

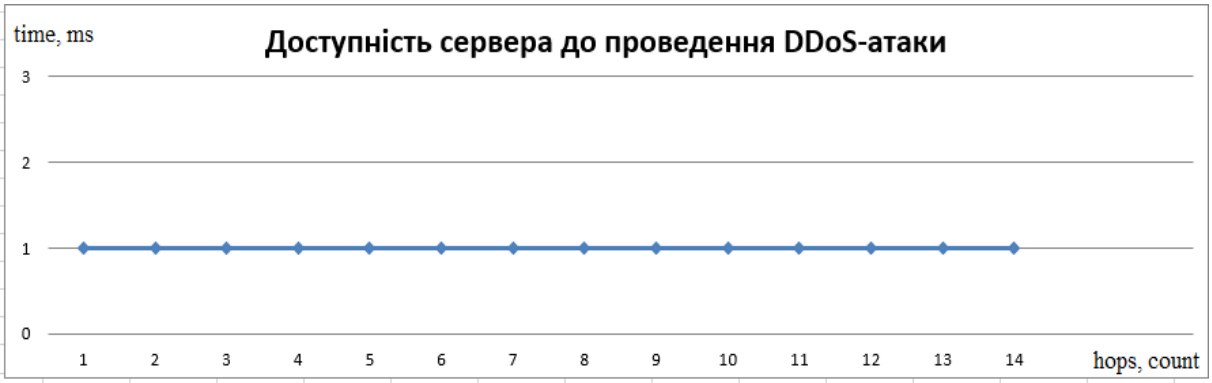

Рис. 19. Графік доступності сервера до проведення DDoS-атаки

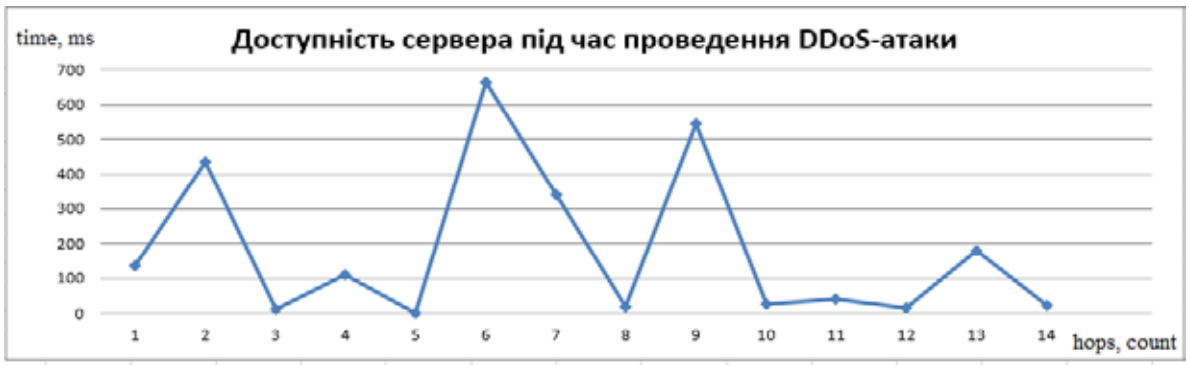

Рис. 20. Графік доступності сервера під час проведення DDoS-атаки

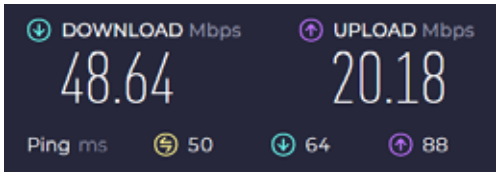

Рис. 21. Перевірка швидкості інтернету під час проведення DDoS-атаки

Вплив DDoS-атаки призвів до збільшення часу відгуку пристроїв локальної мережі:

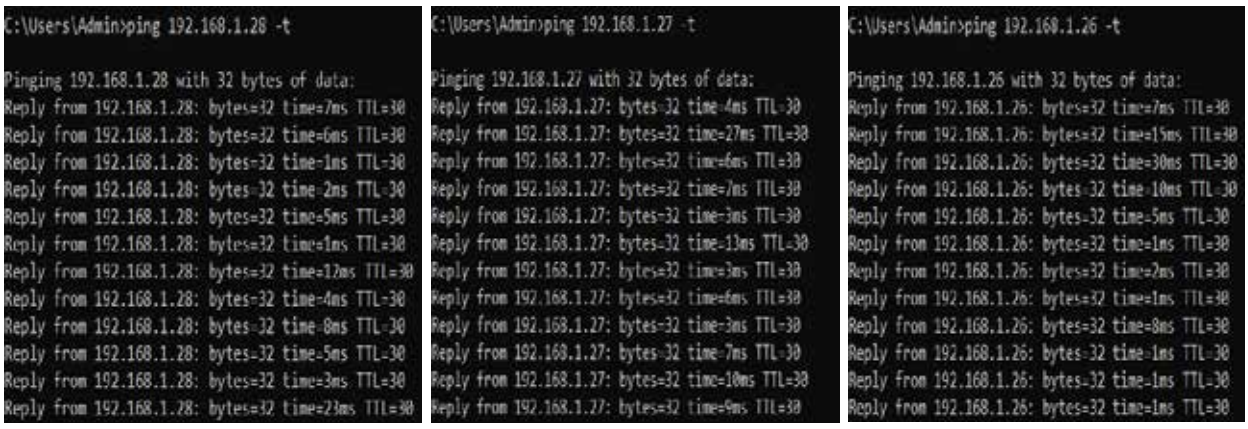

Рис. 22. Перевірка доступності пристроїв під час проведення DDoS-атаки

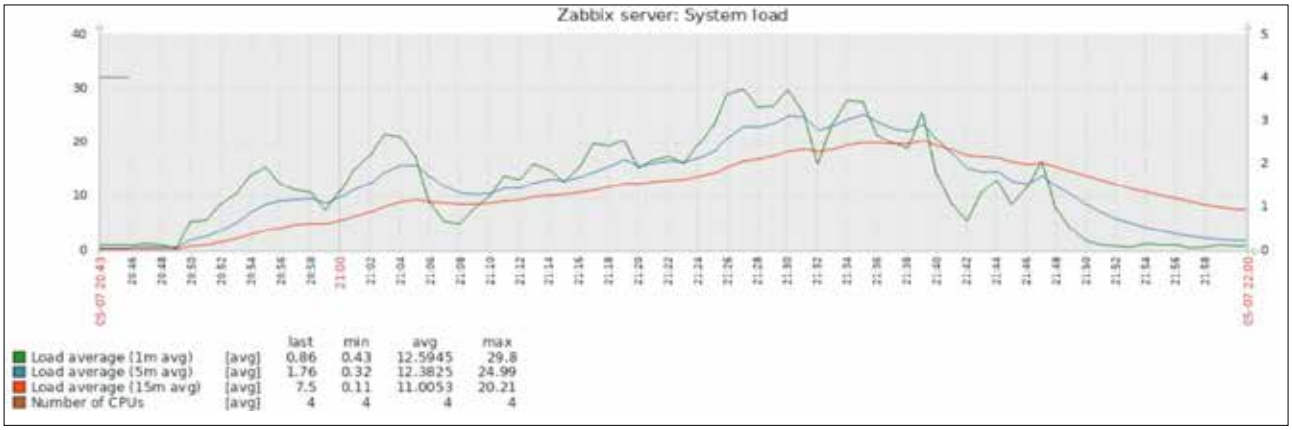

Рис. 23. Графічне відображення завантаженості сервера під час проведення атаки

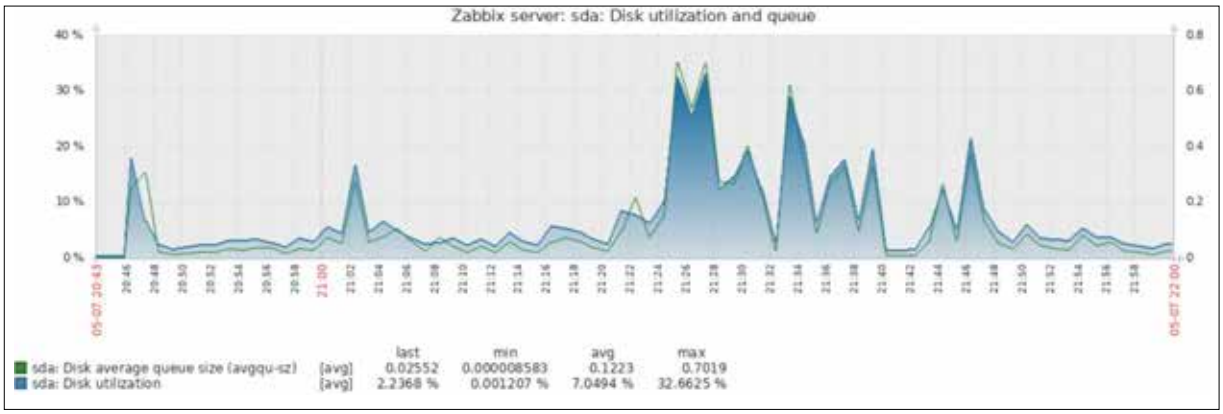

Рис. 24. Графічне відображення використання диску під час проведення атаки

Параметр “system load” відображає середнє навантаження на систему протягом певного часового інтервалу. Коли система перевантажена, “system load” зростає, що може призвести до збільшення часу відгуку сервера, затримок у виконанні запитів та загальної деградації продуктивності, що відображено на рис. 23.

Окрім завантаженості центрального процесора відбулось значне збільшення обсягу оброблюваної інформації. Це впливає на параметр Disk Utilization (використання диска), особливо у випадку використання віртуальної пам’яті (paging) або файлової системи, яка зберігає логи. Збільшення параметру Disk Utilization має вплив на продуктивність сервера, оскільки доступ до даних на диску стає в рази повільнішим, що відображено на рис. 24.

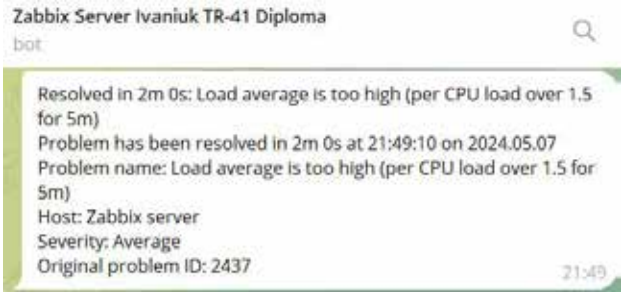

Рис. 25. Реакція чат-бота в телеграмі на стабілізацію трафіку

Після завершення DDoS-атаки сервер надіслав до чат-боту повідомлення про стабілізацію своєї роботи, що свідчить про відновлення його коректного функціонування, що відображено на рис. 25.

Модернізуємо існуючі тригери системи моніторингу Zabbix, задля того, щоб система більш точно класифікувала причину проблеми перенавантаження центрального процесора сервера. Скріншоти модернізації тригерів показані на рис. 26 та рис. 27.

Після проведення повторної DDoS-атаки на сервер, в чат-бот надійшли повідомлення з точнішою класифікацією проблеми, що відображено на рис. 28.

Даний прототип може бути використаний для аналізу мережевих аномалій, тестування нових методів захисту від кіберзагроз, оптимізації мережевого трафіку, автоматизації управління мере-

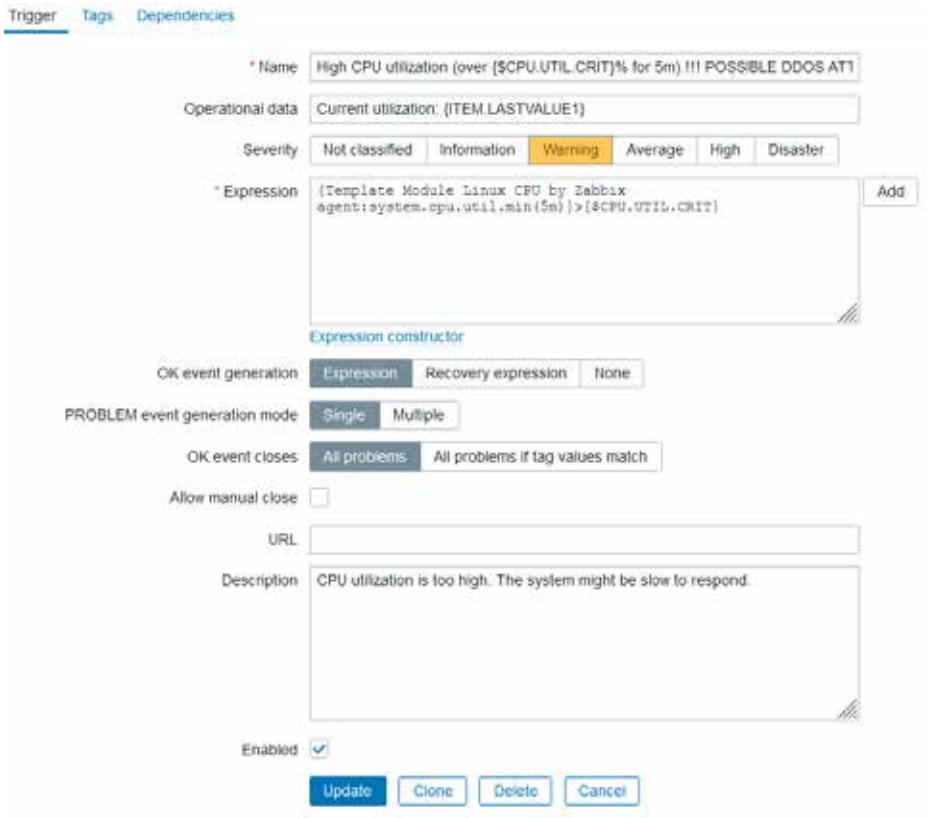

Рис. 26. Модернізація тригера “High CPU Utilization”

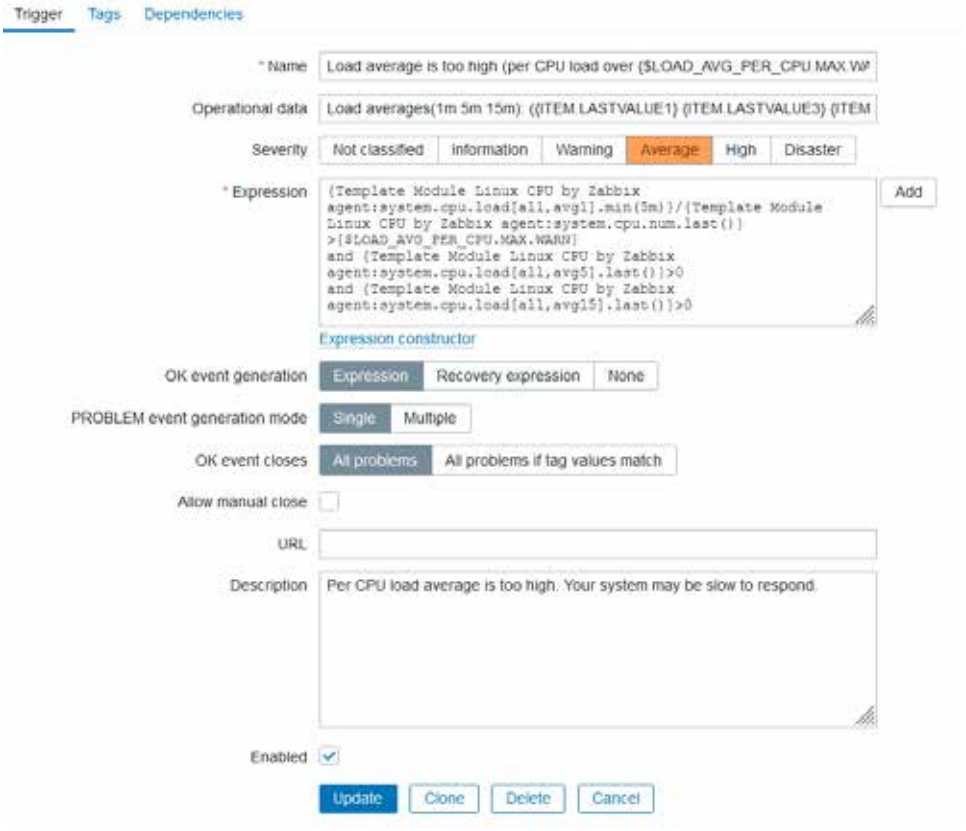

Рис. 27. Модернізація тригера “Load Average is too high”

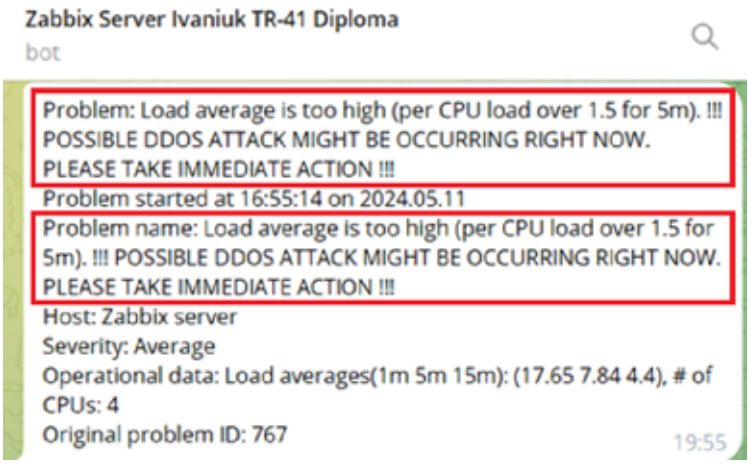

Рис. 28. Результат модернізації тригера "Load Average is too high"

жами та навчання фахівців з адміністрування телекомунікаційних мереж та кібербезпеки. Після успішного тестування запропонованих рішень на прототипі можна впроваджувати удосконалені системи моніторингу в реальні мережі, забезпечуючи їх надійність та ефективність.

Висновки. У роботі створено прототип телекомунікаційної мережі, призначений для випробувань та аналізу систем моніторингу на прикладі Zabbix. Використання прототипу дало можливість проводити безпечні експерименти у контрольованих умовах, мінімізуючи ризики для реальної інфраструктури. Встановлено систему моніторингу Zabbix і реалізовано процедуру автоматичного додавання нових хостів, що значно спрощує інтеграцію нових пристроїв. Розроблено чат-бота в Telegram для оперативного сповіщення адміністраторів про інциденти у мережі, забезпечуючи можливість швидкого реагування на виникнення проблем. Також проведено тестування мережі за допомогою DDoS-атак для оцінки її стійкості, що допомогло виявити слабкі місця у захисті та внести необхідні корективи в існуючі тригери системи, підвищуючи її ефективність і надійність.

Список літератури:

1. Muhati E., Rawat D. Data-Driven Network Anomaly Detection with Cyber Attack and Defense Visualization. *Journal of Cybersecurity and Privacy*. 2024. Vol. 4. № 2. P. 241–263. URL: https://doi.org/10.3390/jcp4020012

2. Mardiyono A., Sholihah W., Hakim F. Mobile-based Network Monitoring System Using Zabbix and Telegram. *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)*, Yogyakarta, 15–16 September 2020. 2020. URL: https://doi.org/10.1109/ic2ie50715.2020.9274582

3. Katonová E. A., Džubák J., Feciľak P. Automated Monitoring of Network Infrastructures Based on the Zabbix Solution. *2023 21st International Conference on Emerging eLearning Technologies and Applications (ICETA)*, Stary Smokovec, Slovakia, 26–27 October 2023. 2023. URL: https://doi.org/10.1109/iceta61311.2023.10344265

4. A comprehensive survey on DDoS defense systems: New trends and challenges / Q. Li et al. *Computer Networks*. 2023. Vol. 233. P. 109895. URL: https://doi.org/10.1016/j.comnet.2023.109895

5. Mohd Fuzi M. F., Mohammad Ashraf N. F., Jamaluddin M. N. F. Integrated Network Monitoring using Zabbix with Push Notification via Telegram. *Journal of Computing Research and Innovation*. 2022. Vol. 7. № 1. P. 147–155. URL: https://doi.org/10.24191/jcrinn.v7i1.282 (date of access: 28.05.2024).

6. Vingestin I., Kalsum T. U., Mardiana Y. The Design Of Network Monitoring System Using SNMP Protocol With Telegram Notification. *Jurnal Media Computer Science*. 2023. Vol. 2. № 1. URL: https://doi.org/10.37676/jmcs.v2i1.3441

Beshley H.V., Ivaniuk M.M., Beshley M.I. **DEVELOPMENT OF A TELECOMMUNICATION NETWORK PROTOTYPE FOR TESTING AND ENHANCING ZABBIX MONITORING SYSTEMS**

This paper presents a prototype network infrastructure designed to research and improve monitoring systems, including Zabbix. The prototype is designed as a testbed that provides a safe environment for experimentation while minimizing the risks to real-world infrastructure. The relevance of the study is due to

the need for a quick and effective response to anomalies and threats in telecommunications networks using monitoring systems.

The prototype network infrastructure includes network equipment such as routers, switches, and servers integrated with the Zabbix monitoring system. A virtual machine with expanded RAM and a network connection in bridge mode was configured, providing a stable environment for testing. Zabbix monitoring system with an automated procedure for adding new hosts was installed, which greatly simplifies network management and integration of new devices. Integration of the Telegram chatbot into the monitoring system allowed us to automatically send incident notifications to administrators, increasing the efficiency of problem response. To analyze the system's resistance to DDoS attacks, we created a script in the C programming language and tested it in the Termux environment. The testing demonstrated the system's ability to detect and respond to various types of attacks and identified weaknesses in the protection. Modernization of the triggers for detecting network anomalies has increased the efficiency of responding to threats and allowed for timely detection of problems. This approach makes it possible to identify and eliminate potential threats at an early stage, which is important for ensuring the reliability and security of telecommunications systems.

Future work involves further improving the monitoring system using machine learning algorithms for analytics and decision-making, expanding the functionality of the chatbot and automated procedures, and conducting additional testing to improve the reliability and security of telecommunications networks. The company plans to study the impact of various types of cyber threats and develop new methods for detecting and neutralizing them.

Key words: *monitoring system, telecommunications network prototype, DDoS attack simulation, triggers, anomaly detection, reliability, threat response.*