УДК 621.391

к.т.н. **Погребняк Л.М.** (ІСЗЗІ, м. Київ)
Лукіна К.В. (ІСЗЗІ, м. Київ)

DOI: http://doi.org/10.17721/2519-481X/2025/87-11

АНАЛІЗ ЗАСОБІВ МОНІТОРИНГУ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ

У статті розглянуто актуальні питання моніторингу електронних комунікаційних мереж в умовах стрімкого розвитку інформаційних технологій, зростання кіберзагроз та особливостей функціонування мережевої інфраструктури під час воєнного стану.

Основну увагу приділено аналізу сучасних програмно-апаратних інструментів, що використовуються для контролю за працездатністю та безпекою електронних комунікаційних мереж, а також для оперативного виявлення перевантажень, збоїв, аномалій і потенційно небезпечної активності.

Проведено порівняльний аналіз сучасних інструментів мережевого моніторингу провідних виробників комунікаційного обладнання, зокрема Cisco, MikroTik, Juniper, Ubiquiti, Grandstream. Показано, що запропоновані ними інструменти забезпечують ефективний функціонал, автоматизацію оновлень, гнучкі засоби аналізу даних та підтримку, однак мають обмежені можливості інтеграції з пристроями інших виробників. Це ускладнює впровадження централізованих систем моніторингу в мережах зі змішаною структурою.

Розглянуто також незалежні універсальні системи моніторингу, такі як Zabbix, Nagios, NeDi, PRTG Network Monitor, Cacti, Wireshark, які мають змогу взаємодіяти з широким спектром різнотипного мережевого обладнання за допомогою відкритих протоколів (SNMP, HTTP/HTTPS API, ICMP). Показано переваги таких систем у контексті масштабованості, адаптивності та гнучкості конфігурації.

Обґрунтовано доцільність гібридного підходу до побудови систем моніторингу, який поєднує функціональні можливості вендорних і незалежних рішень, що дозволяє досягти високого рівня деталізації даних та їхню візуалізацію, здійснювати оперативну аналітику в реальному часі, формувати ефективну систему реагування на інциденти, а також забезпечити високу стійкість гетерогенної мережі до зовнішніх впливів і кіберзагроз.

Ключові слова: моніторинг, інструменти та системи моніторингу, управління мережею, сервіси, мережеві ресурси, безпека.

Вступ та постановка проблеми. В умовах воєнного стану електронні комунікаційні мережі (ЕКМ) відіграють ключову роль у забезпеченні функціонування державних органів та управлінні критичною інфраструктурою. Разом з тим суттєву загрозу національній безпеці та інформаційному просторі України становлять атаки на електронну комунікаційну мережу.

Ефективне функціонування державних органів як у військовий, так і в мирний час потребує постійного вдосконалення технологій та засобів ЕКМ. Стрімкий розвиток елементної бази, а відповідно і засобів побудови мереж, та наукові досягнення в області електронних комунікацій, що стимулюють швидкий розвиток технологій, ускладнюють процеси передачі інформації та вимагають удосконалення систем моніторингу та управління. Своєчасне виявлення та реагування на інциденти в ЕКМ дозволяє забезпечити допустиму якість зв’язку та підтримувати функціонування критичних сервісів навіть в умовах надзвичайних ситуацій, а також запобігти масштабним технічним збоям та витоку інформації, які в свою чергу сприяють підриву обороноздатності держави.

ЕКМ функціонують із використання обладнання різних фірм виробників, які мають різноманітні набори інструментів моніторингу, що стає на заваді здійсненню моніторингу мережі в цілому.Відповідно до переліку заходів "Стратегії розвитку сфери електронних комунікацій України на період до 2030 року" [1] триває процес розробки та впровадження універсальної комплексної системи моніторингу, тому аналіз існуючих інструментів

моніторингу фірм виробників основного комунікаційного обладнання та систем моніторингу є актуальним завданням.

Аналіз останніх досліджень і публікацій. В [2 - 5] сформульовано основні завдання, вимоги та підходи до моніторингу електронних комунікаційних мереж.

В [6,7] було здійснено дослідження методів активного та пасивного моніторингу, розглянуто декілька систем мережевого моніторингу (Zabbix, Wireshark).

В [8] розглянуто систему моніторингу Prometheus та запропоновано підходи до збору та аналізу метрик на базі цієї системи моніторингу.

В [9] розглянуто системи моніторингу PRTG, Nagios, Zabbixта можливість інтеграції їх в електронні комунікаційні мережі.

У результаті аналізу досліджень і публікацій встановлено, що проблема моніторингу електронних комунікаційних мереж (ЕКМ) залишається надзвичайно актуальною в умовах стрімкого зростання обсягів переданих даних, ускладнення мережевої інфраструктури, підвищення вимог до її надійності, продуктивності та кібербезпеки. Ці виклики додатково ускладнюються впровадженням новітніх мережевих архітектур, зокрема мереж, побудованих за концепціями програмно-орієнтованих мереж (SDN), віртуалізації мережевих функцій (NFV), хмарних рішень та мобільних мереж п’ятого покоління (5G), що вимагає принципово нових підходів до моніторингу та управління.

Існує широкий спектр програмних і апаратних засобів моніторингу, кожен з яких орієнтований на певні аспекти функціонування мережі − трафік, доступність, продуктивність, виявлення аномалій та кіберзагроз.

Отже, доцільним є детальний аналіз сучасних засобів моніторингу електронних комунікаційних мереж з метою виявлення їх функціональних можливостей, переваг, недоліків і потенціалу до інтеграції в складні багаторівневі мережеві інфраструктури. Це дозволить обґрунтувати вибір або розробку найбільш ефективних засобів моніторингу для конкретних умов експлуатації мереж.

Метою статті є: аналіз інструментів моніторингу різнотипного комунікаційного обладнання ЕКМ та систем моніторингу мережі.

Виклад основного матеріалу. Моніторинг електронних комунікаційних мереж є ключовим елементом забезпечення надійності, продуктивності та інформаційної безпеки в умовах зростання складності та масштабу сучасних інформаційно-комунікаційних систем. Він здійснюється із застосуванням спеціалізованого апаратного й програмного забезпечення та охоплює широкий спектр задач: контроль працездатності мережевого обладнання (інфраструктурний моніторинг); оцінювання ефективності функціонування веб-сервісів, хмарних платформ і прикладних компонентів (моніторинг продуктивності додатків); аналіз мережевого трафіку для виявлення аномальних активностей, перевантажень і збоїв (моніторинг трафіку); виявлення потенційних загроз, атак і несанкціонованих втручань (моніторинг безпеки).

Залежно від підходу до збору інформації, розрізняють активний та пасивний моніторинг. Активний моніторинг передбачає генерування контрольних (тестових) запитів до мережевих елементів (наприклад, ping, traceroute, SNMP-запити) для діагностики їхнього стану та вимірювання параметрів, таких як затримка, доступність і пропускна здатність. Пасивний моніторинг базується на неінвазивному аналізі реального мережевого трафіку для виявлення прихованих загроз, порушень політик безпеки, а також визначення характеру та інтенсивності навантаження на мережеву інфраструктуру.

За масштабом охоплення виділяють локальний моніторинг, який обмежується внутрішньою інфраструктурою організації, та глобальний моніторинг, що охоплює розподілені мережеві ресурси, включаючи хмарні обчислювальні середовища та мережі загального користування (рис.1).

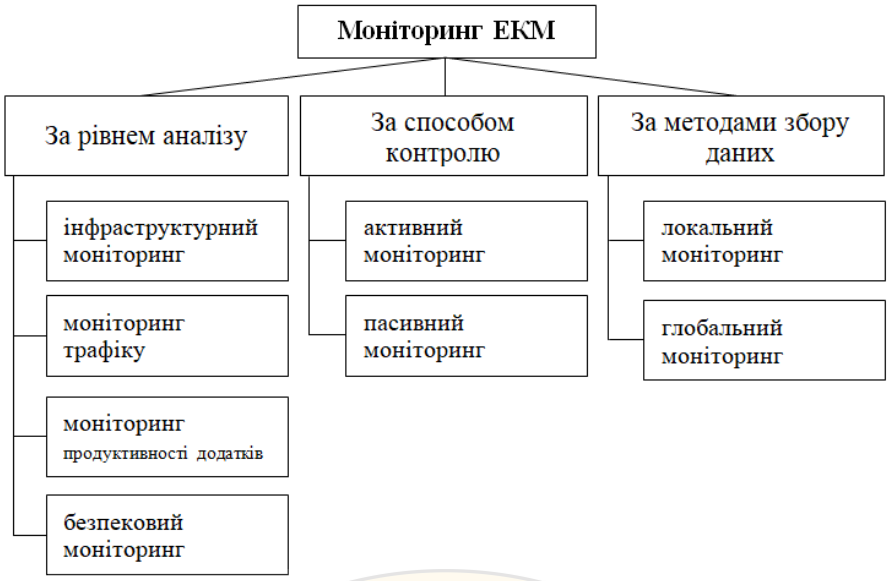

Рисунок 1 – Типи моніторингу в електронних комунікаційних мережах

Моніторинг ЕКМ може здійснюватися як за допомогою вбудованих інструментів моніторингу, що надаються виробниками обладнання, так і з використанням сторонніх систем керування мережею.

У випадку використання обладнання компанії Cisco [10], доступний широкий спектр інструментів для моніторингу, управління та аналітики мережевої інфраструктури, деякі з них представлені в табл. 1.

Таблиця 1

Інструменти управління та моніторингу обладнання Cisco

Назва	Призначення	Переваги	Недоліки
Cisco Prime Infrastructure	комплексна платформа для управління мережами, яка включає функції моніторингу, управління конфігураціями, автоматизації та аналітики для пристроїв Cisco	– можливість автоматизації та конфігурації процесів налаштування мережі; – наявність інструментів для глибокого аналізу продуктивності; – зручний, інтуїтивно зрозумілий інтерфейс користувача.	– висока вартість (особливо для невеликих або середніх компаній); – складність налаштування; – підтримка лише пристроїв Cisco.
Cisco DNA Center	платформа для управління та автоматизації мережі на основі програмного забезпечення, яка включає функції моніторингу та аналізу продуктивності для мереж Cisco	– можливість автоматизації та конфігурації процесів налаштування мережі; – наявність інструментів для глибокого аналізу продуктивності; – зручний, інтуїтивно зрозумілий інтерфейс користувача; – інтеграція з іншими рішеннями Cisco (напр. Cisco Meraki).	– висока вартість (особливо для невеликих компаній); – складність налаштування та використання; – підтримка лише пристроїв Cisco (підтримка інших пристроїв дуже обмежена).
Cisco Meraki Dashboard	система для моніторингу та управління пристроями Meraki (які належать Cisco), таких як маршрутизатори, точки доступу Wi-Fi, комутатори тощо	– хмарне управління; – зручний, інтуїтивно зрозумілий інтерфейс користувача; – автоматичне оновлення програмного забезпечення на всіх пристроях; – можливість моніторингу мережі в реальному часі.	– обмежена гнучкість в порівнянні: з іншими рішеннями Cisco; – залежність від Інтернету; – обмежена підтримка сторонніх пристроїв.

Назва	Призначення	Переваги	Недоліки
Cisco NetFlow Analyzer	інструмент для моніторингу та аналізу трафіку в мережах, який використовує технологію NetFlow для збору метрик трафіку	– глибокий аналіз трафіку; – масштабованість; – інтеграція з іншими рішеннями Cisco.	– складність налаштування; – підходить не для всіх типів мереж (найкраще працює для мереж, що підтримують Net Flow).

Для обладнання компанії Grandstream [11] застосовується низка інструментів моніторингу та централізованого управління, що забезпечують ефективне адміністрування мережевої інфраструктури, а також підвищують рівень доступності та безпеки сервісів (табл.2). Вибір інструменту залежить від типу обладнання та функціонального призначення:

Grandstream Device Management System (GDMS) − хмарна платформа, яка дозволяє централізовано керувати великою кількістю IP-телефонів, шлюзів та IP-АТС. Вона забезпечує віддалене налаштування, оновлення прошивок, моніторинг стану пристроїв у реальному часі та спрощене впровадження нових рішень у корпоративних мережах;

GWN Cloud / GWN Manager − інструменти управління для Wi-Fi точок доступу, маршрутизаторів та комутаторів серії GWN:

GWN Cloud – це безкоштовна хмарна система, яка дозволяє контролювати всю інфраструктуру з будь-якої точки світу через зручний веб-інтерфейс або мобільний застосунок;

GWN Manager – локальна альтернатива хмарному сервісу, яка надає аналогічний функціонал для організацій, що віддають перевагу розгортанню рішень у власному середовищі;

UCM Remote Connect – рішення для безпечного віддаленого доступу та адміністрування IP-АТС серії UCM6300. Інтегрується з GDMS та дозволяє здійснювати віддалену підтримку, моніторинг дзвінків, налаштування функцій зв’язку, маршрутизацію викликів та забезпечення резервування.Такий набір інструментів створює гнучку, масштабовану та безпечну екосистему для керування як невеликими локальними інсталяціями, так і складними багаторівневими мережевими структурами.

Таблиця 2

Інструменти управління та моніторингу обладнання Grandstream

Назва	Призначення	Переваги	Недоліки
Grandstream Device Management System	хмарна система керування та моніторингу для VoIP-пристроїв Grandstream, зокрема телефонів, шлюзів та IP-АТС.	– хмарне управління без потреби у локальному сервері; – центральне налаштування та оновлення пристроїв; – моніторинг статусу пристроїв у реальному часі, Push-сповіщення про збої в роботі та оновлення; – безкоштовний доступ.	– залежність від інтернет-з'єднання; – обмежена підтримка пристроїв (не всі моделі сумісні); – можливості порівняно з локальними рішеннями.
GWN Cloud	хмарний сервіс для управління мережевими пристроями Grandstream GWN (Wi-Fi точки доступу, комутатори, та маршрутизатори).	– центральне керування мережами з будь-якої точки світу – автоматичне оновлення прошивки – наявність інструментів для глибокої аналітика та звітності – безкоштовний сервіс	– відсутність локального резервного варіанту (окрім GWN Manager); – обмежений контроль у порівнянні з професійним рішеннями (наприклад, Cisco Meraki).

Назва	Призначення	Переваги	Недоліки
GWN Manager	локальне програмне забезпечення для управління мережею Wi-Fi Grandstream без потреби в хмарних сервісах.	– працює без підключення до інтернету; – вищий рівень безпеки; – можливість масштабування	– складність налаштування; – потрібен окремий сервер для роботи.
Grandstream UCM Remote Connect	хмарна система для безпечного підключення віддалених VoIP-користувачів до IP-АТС UCM6300.	– захищений тунель без складних VPN-налаштувань; – просте підключення віддалених телефонів; – інтеграція з GDMS.	– залежність від хмарної інфраструктури; – обмежена підтримка для старих моделей UCM.

В екосистемі MikroTik [12] реалізовано потужні інструменти для моніторингу та аналізу мережевої інфраструктури, які забезпечують гнучке керування та високу прозорість мережевих процесів (табл.3):

Dude – інтелектуальна система централізованого моніторингу мережі, яка автоматично виявляє пристрої, створює візуальну топологію мережі та надає детальну інформацію про статус обладнання в режимі реального часу. Завдяки зручному графічному інтерфейсу адміністратор отримує повний контроль над структурою та станом мережі.

Traffic Flow – вбудований механізм для збору, аналізу та передачі статистики про мережевий трафік. Підтримує стандарти Net Flow, sFlow та інші формати, що дає змогу інтегрувати MikroTik з професійними системами аналізу трафіку та забезпечити глибоке розуміння навантаження на мережу, виявлення аномалій і оптимізацію її роботи.

Ці інструменти є невід'ємною частиною професійного середовища для адміністрування мультисервісних мереж на базі рішень MikroTik.

Таблиця 3

Інструменти управління та моніторингу обладнання MikroTik

Назва	Призначення	Переваги	Недоліки
Dude	система моніторингу, яка забезпечує автоматичне виявлення пристроїв мережі, має **гр**афічний інтерфейс для візуалізації мережі**,** здійснює **м**оніторинг за допомогою SNMP, ICMP	– безкоштовний; – зручний графічний інтерфейс; – гнучка система сповіщень; – автоматичне виявлення пристроїв; – можливість моніторингу не тільки пристроїв MikroTik, але й SNMP-сумісних мережевих пристроїв.	– працює тільки на Windows; – обмежена масштабованість; – негнучка система аналітики та звітів; – обмежені можливості збору метрик.
Traffic Flow	реалізація технології NetFlow, яка дозволяє здійснювати аналіз трафіку в мережі	– глибокий аналіз трафіку; – вбудований в RouterOS; – може працювати з PRTG та Wireshark.	– високе споживання ресурсу; – не використовується в малопотужних пристроях MikroTik (можуть бути затримки)

Компанія Juniper Networks надає широкий спектр програмних рішень для моніторингу, управління та аналітики мережевої інфраструктури, орієнтованих як на традиційні, так і на віртуалізовані середовища (табл.4) [13].

Таблиця 4

Інструменти управління та моніторингу обладнання Juniper

Назва	Призначення	Переваги	Недоліки
Junos OS	призначена для управління мережевим обладнанням.	– містить вбудовані інструменти для моніторингу та діагностики; – підтримує SNMP, що	– потребує певних знань для встановлення та роботи – висока вартість обладнання Juniper

Назва	Призначення	Переваги	Недоліки
		забезпечує можливість інтеграції з іншими системами моніторингу.	
J-Web GUI	веб-інтерфейс, призначений для управління мережевим обладнанням Juniper, працює в Junos OS	– веб-інтерфейс, який є альтернативою командному рядку; – інтуїтивно зрозумілий інтерфейс – легко впроваджуються зміни подачі інформації.	– обмежений функціонал порівняно з CLI, не всі можливості Junos OS доступні – відсутня підтримка всіх CLI-команд – не підходить для великих мереж.
Контролери управління безпроводовими мережами WLM	призначені для централізованого управління, моніторингу безпроводових мереж	– управління здійснюється через хмару; – здатність до масштабування; – можливість планувати, розгортати, оптимізувати та відстежувати бездротові мережі, для ефективного управління та моніторингу Wi-Fi мереж.	– не підходить для закритих систем та систем без інтернету; – висока вартість та витрати на обслуговування.

Основі інструменти управління та моніторингу обладнання Ubiquiti [14] наведено в табл. 5. Ці засоби охоплюють повний спектр функціональності для побудови, адміністрування, діагностики та масштабування як локальних, так і розподілених мережевих систем. Програмні продукти компанії орієнтовані на спрощення процесів налаштування та централізованого управління, забезпечують інтеграцію з хмарними сервісами, а також підтримку автоматизованого виявлення несправностей і аналізу продуктивності. Вони адаптовані до різних типів обладнання – від точок доступу і маршрутизаторів серії UniFi до безпроводових операторських рішень на базі AirMAX і AirFiber, що дозволяє Ubiquiti залишатися одним із лідерів у сегменті доступних та ефективних мережевих рішень.

Таблиця 5

Інструменти управління та моніторингу обладнання Ubiquiti

Назва	Призначення	Переваги	Недоліки
UniFi Network Application	програмний комплекс для управління мережевими пристроями Ubiquiti UniFi	– гнучка система сповіщень – може працювати у хмарі; – наявність інструментів для глибокого моніторингу; – автоматичне виявлення пристроїв; – безкоштовна	– обмежена підтримка пристроїв; – немає інтеграції з SNMP; – не підходить для ISP; – для постійного моніторингу необхідний виділений сервер
UISP (Ubiquiti Internet Service Provider)	програмне рішення для використання інтернет-провайдерами	– гнучка система сповіщень; – безкоштовна; – може працювати в хмарі; – наявність інструментів для глибокого аналізу мережі; – централізоване управління	– підтримка лише обладнання Ubiquiti; – для роботи необхідний окремий сервер

Отже, інструменти моніторингу, що розробляються безпосередньо виробниками комутаційного обладнання, безперечно є ефективними у межах відповідної екосистеми. Вони забезпечують глибоку інтеграцію з апаратною частиною, розширені функції керування, діагностики, автоматичного оновлення та підтримки. Проте, ключовим обмеженням таких рішень залишається їх вузька сумісність: більшість із них не підтримують повноцінну інтеграцію з обладнанням інших виробників або потребують складної адаптації для

забезпечення міжвендорної взаємодії. Це суттєво обмежує можливості централізованого моніторингу в гетерогенних мережах, де використовується обладнання різних брендів. Тому, у складних мультивендорних інфраструктурах доцільно застосовувати незалежні або універсальні системи моніторингу, що розроблені для роботи з широким спектром мережевих пристроїв та забезпечують ширшу інтеграцію, гнучкість конфігурації та єдину точку контролю мережевих процесів.

Такі системи не лише забезпечують сумісність на міжвендорному рівні, а й дозволяють працювати у режимі реального часу, виконувати аналіз журналів подій, здійснювати детальну візуалізацію трафіку, а також генерувати інтелектуальні сповіщення у разі виникнення критичних інцидентів. Однак, на відміну від вбудованих фірмових рішень, незалежні платформи − такі як *Zabbix, Nagios, NeDi, PRTG Network Monitor, Cacti, Wireshark* тощо − надають змогу здійснювати моніторинг і централізоване управління різнотипними пристроями мережі з єдиного інтерфейсу, що є особливо цінним для підтримки великих та різнорідних інфраструктур.

Принцип взаємодії систем моніторингу з обладнанням різних виробників базується на використанні універсальних протоколів і стандартів передачі даних, які підтримуються більшістю сучасних мережевих пристроїв. Найпоширенішими серед них є SNMP (Simple Network Management Protocol), HTTP/HTTPS API, ICMP (Internet Control Message Protocol), а також спеціалізовані експортуючі агенти та телеметричні сервіси, реалізовані в інфраструктурі окремих виробників. Завдяки цьому забезпечується ефективна взаємодія між мультивендорним обладнанням та незалежними системами моніторингу, навіть у складних і неоднорідних мережах.

Проведемо аналіз функціональних можливостей найбільш поширених універсальних системи моніторингу, які успішно використовуються для контролю та управління інфраструктурою в умовах технологічного різноманіття (табл. 6).

Таблиця 6

Функціональні можливості незалежних систем моніторингу

Тип моніторингу / Система моніторингу	за рівнем аналізу				за методами збору даних				підтримка ОС	
	Інфраструктурний моніторинг	Моніторинг трафіку	Моніторинг продуктивності додатків	Безпековий моніторинг	Активний моніторинг	Пасивний моніторинг	Локальний моніторинг	Глобальний моніторинг	Windows	Linux
Zabbix	+	+	+	+	+	+	+	+	+	+
Nagios	+	+	+	+	+	+	+	+	+	+
NeDi	–	–	+	+	+	+	+	–	+	+
Wireshark		+	–	+	–	+	–	–	+	+
PRTG	+	+	+	+	+	+	+	+	+	–
Prometheus	+	–	+	–	+	+	+	–	+ (через Docker)	+
Observium	+	–	–	–	+	+	–	–	+	+
Kismet	–	–	–	+	–	+	+	–	–	+
Cacti	+	+	–	–	–	+	+	–	+*	+
Network Olympus	–	–	–	–	+	+	+	–	+	–

Примітка. Позначення: «+» – підтримує, «–» – не підтримує або не підтримує напряму, «+* » – підтримує при додаткових налаштуваннях.

Універсальна система моніторингу Zabbix забезпечує детальний контроль стану мережевого обладнання, серверів і додатків. Вона підтримує SNMP, IPMI, WMI та

агентський моніторинг. Zabbix має гнучку систему сповіщень, аналітику за рахунок збереження історії та можливість автоматизації типових завдань [9, 15-17].

Потужна система моніторингу Nagios дозволяє контролювати стан серверів, мережевого обладнання, додатків і служб. Підтримує агентний і безагентний методи збору даних, що дозволяє використовувати її в різних середовищах. Nagios може надсилати сповіщення адміністраторам у разі виявлення проблем, а також автоматично виконувати дії для їх усунення. Завдяки підтримці великої кількості плагінів система легко адаптується до специфічних потреб організацій [9, 18, 19].

Програмне забезпечення NeDi сканує мережу за MAC, IP та DNS адресами і створює власну базу даних. Дозволяє використовувативеб-інтерфейс для взаємодії з користувачем, що надає можливість здійснювати онлайн-моніторинг усіх фізичних пристроїв та їх розташування у вашій локальній мережі [20].

Рішення для комплексного моніторингу мережі PRTG Network Monitor сумісне з пристроями Windows, підтримує NetFlow, SNMP, WMI. Має інтуїтивно зрозумілий інтерфейс, вбудовані сенсори для моніторингу трафіку, серверів, сховищ даних та віртуальних машин. PRTG дозволяє створювати детальні графіки продуктивності, налаштовувати автоматичні сповіщення та аналізувати пропускну здатність мережі [9, 21].

Система моніторингу Cacti, яка підтримує SNMP, призначена для візуалізації стану обладнання та лінії зв'язку на різних рівнях мережі передачі даних за допомогою розвиненої системи побудови графіків для моніторингу параметрів. Cacti має повністю розподілену та стійку до збоїв структуру збору даних, розширені функції автоматизації на основі шаблонів для пристроїв та графіків, кілька методів збору даних, можливість розширення за допомогою плагінів функцій керування користувачами, групами та доменами на основі ролей [22].

Аналізатор мережевих пакетів Wireshark дозволяє перехоплювати та аналізувати мережевий трафік в режимі реального часу, здійснювати аналітику безпеки. Він не є повнофункціональною платформою моніторингу, яка збирає та аналізує дані в масштабі всієї мережі. Wireshark ідеально інтегрується з системами на базі *NIX, Windows та macOS [7].

Система моніторингу Observium працює з використанням протоколу SNMP та підтримує широкий спектр типів пристроїв, платформ і операційних систем, включаючи Windows, Linux, HP, Juniper, Cisco, Dell, FreeBSD та інші. Цей додаток дозволяє моніторити мережу в режимі реального часу, оцінити стан та продуктивність мережі та мережевого обладнання. В Observium доступні версії Community (безкоштовна) та Professional (платна) [15, 23].

Сучасна система моніторингу Prometheus, розроблена для збору метрик у хмарних середовищах та контейнеризованих інфраструктурах. Вона використовує базу даних time-series, що дозволяє зберігати та аналізувати збережені дані про продуктивність систем. Завдяки підтримки мови запитів PromQL Prometheus має можливість виконувати складний аналіз метрик, робитигнучкі запити та сповіщення в режимі реального часу. Для візуалізації даних Prometheus часто використовується разом із Grafana, що є ефективним рішенням для компаній, які працюють із мікросервісною архітектурою [24].

Система моніторингу мережі **Network Olympus** призначена для моніторингу стану пристроїв та служб, які потребують постійного контролю, що забезпечує працездатність системи, своєчасно виявляти потенційні проблеми та ефективно вирішувати їх, виконуючи різні сценарії та дії, надаючи докладні звіти про будь-які збої. Основною особливістю Network Olympus є наявність конструктора сценаріїв, який допомагає організувати схему моніторингу практично будь-якої складності для точного виявлення проблем та збоїв, а також автоматизувати їх усунення [15, 20].

Додаток Kismet який призначений для аналізу трафіку в безпроводових локальних мережах, а також дозволяє виявляти незаконні точки доступу, інші приховані пристрої [25, 26].

Більшість систем підтримує операційні системи Windows та Linux, принаймні через

SNMP чи інші протоколи. Для ОС Windows доцільніше використовувати Dude та PRTG, а для ОС Linux – Kismet, Network Olympus.

Значна частина систем моніторингу розповсюджуються з відкритим вихідним кодом і є безкоштовними. Однак, PRTG безкоштовний для незначної (до 10) кількості пристроїв, а масштабування мережі потребує використання платної версії системи. Observium доступний безкоштовно лише з обмеженим функціоналом, повний функціонал – платний. Складними системами моніторингу для налаштування та обслуговування вважаються Observium, Nedi, Kismet та Zabbix. Система Zabbix може здійснювати різні види моніторингу всієї інфраструктури, ефективно працювати при масштабуванні мережі. Вона розповсюджується безкоштовно, проте має складний інтерфейс, досить складна в налаштуванні та обслуговуванні. Окрім Zabbix, системи моніторингу Prometheus, Nagios, Observium та PRTG (платна версія) також гарно себе зарекомендували при роботі з великою кількістю мережевих пристрої.

Візуалізація процесів моніторингу представлена в усіх системах, але в Prometheus вона налаштовується досить складно.

Моніторинг в реальному часу (з затримками в кілька секунд) здійснюється Wireshark, Kismet, Network Olympus, NeDi, Dude та PRTG, з інтервалом до хвилина – Zabbix, Prometheus та Nagios, а з інтервалом до 5-10 хвилин – Cacti та Observium.

Більшість систем моніторингу функціонують з усією мережевою інфраструктурою, однак для здійснення пасивного аналізу трафіку безпроводових мереж Wi-Fi доцільно застосовувати Kismet, для активного аналізу –Wireshark. Для моніторингу систем з хмарною інфраструктурою необхідно застосовувати Prometheus, який підтримує моніторинг out-of-the-box.

Висновки. Моніторинг електронних комунікаційних мереж є критично важливою складовою забезпечення їх надійного, продуктивного та безпечного функціонування. Проведений аналіз інструментів моніторингу різнотипного комунікаційного обладнання ЕКМ та систем моніторингу мережі показав, що розмаїття технологічних рішень, представлених на ринку, дає змогу ефективно адаптувати системи моніторингу до різних масштабів і специфіки мережевих інфраструктур – від локальних корпоративних мереж до розподілених хмарних середовищ.

Інструменти моніторингу фірм виробників комунікаційного обладнання та окремі рішення для мультивендерних мереж дозволяють здійснювати контроль за станом обладнання, виявляти перевантаження та несправності, аналізувати трафік, що забезпечує підвищення продуктивності, надійності та інформаційної безпеки. Показано, що найкращим рішенням є застосування комплексу інструментів та рішень моніторингу для попередження або виявлення проблем, що можуть виникнути під час роботи мережі, на самих ранніх стадіях.

Вибір конкретного рішення має ґрунтуватися на таких факторах, як: архітектура мережі, вимоги до безпеки, бюджет, технічна кваліфікація персоналу, наявність сумісного обладнання та необхідність підтримки сторонніх пристроїв.

Отже, для досягнення високого рівня керованості та надійності ЕКМ доцільно впроваджувати інтегровані системи моніторингу, які поєднують гнучкість налаштувань, можливість аналітики у реальному часі та підтримку сучасних стандартів збирання та обробки мережевих даних. Надалі варто здійснити дослідження щодо побудови гібридних систем моніторингу із застосуванням методів штучного інтелекту та машинного навчання для автоматизованого виявлення аномалій та прогнозування збоїв у мережах.

ЛІТЕРАТУРА:

1. Стратегія розвитку сфери електронних комунікацій України на період до 2030 року. Міністерство цифрової трансформації України. https://thedigital.gov.ua/storage/uploads/files/Стратегія:15:05.pdf

2. М.Г. Треньов, А.Г. Прокопенко Основні принципи роботи та вимоги до створення структур перспективних систем моніторингу розподілених інформаційно-телекомунікаційних мереж / Телекомунікаційні та інформаційні технології, 2024. № 3(84), С.77-85, https://doi.org/10.31673/2412-4338.2024.037785

3. Контроль якості електронних комунікаційних послуг. Технології та процедури. Український державний центр радіочастот. https://www.ucrf.gov.ua/pres-centr/news/kontrol-iakosti-elektronnykh-komunikatsiinykh-posluh-tekhnolohii-ta-protsedury.

4. Сучасний стан, проблеми і перспективи розвитку в Україні електронних адміністративних послуг Аналітична записка. / Інститут стратегічних досліджень. https://www.niss.gov.ua/doslidzhennya/politika/suchasniy-stan-problemi-i-perspektivi-rozvitku-v-ukraini-elektronnikh

5. П.Ю. Паталашко, Н.І. Кушніренко, Н.Г. Козаченко, Н.В. Бойко Розробка системи моніторингу подій інформаційної безпеки / Інформатика та математичні методи в моделюванні, 2023. Том13, № 3-4, С. 282-292. https://DOI 10.15276/imms.v13.no3-4.282

6. І.В. Касовська, О.Д. Шаповаленко, І.М. Луценко Програмні комплекси мережевого моніторингу для підвищення ефективності захисту мереж / Сучасний захист інформації, 2021. №1(45), С. 47-52. https://DOI: 10.31673/2409-7292.2021.014757

7. Jakub Svoboda, Ibrahim Ghafir and Vaclav Prenosil Network Monitoring Approaches: An Overview / International Journal of Advances in Computer Networks and Its Security – IJCNS, 2015. Vol.5, issue 2, p. 88-93. https://www.researchgate.net/profile/Ibrahim_Ghafir/publication/305957483_Network_Monitoring_Approaches_An_Overview/links/57a75c9d08aefe6167bc1f91/Network-Monitoring-Approaches-An-Overview.pdf

8. Inna Stetsenko, Anton Myroniuk Software for collecting and analyzing metrics in the highly loaded applications based on the Prometheus monitoring system / *Information, Computing and Intelligent Systems*, 2024. № 5, p. 17–28. https://doi.org/10.20535/2786-8729.5.2024.316366

9. Atish Barhate Comparison of Network Monitoring Tools: PRTG, SolarWinds, Nagios, Zabbix, and Datadog [Електронний ресурс] Режим доступу: https://www.linkedin.com/pulse/comparison-network-monitoring-tools-prtg-solarwinds-nagios-atish-b-26bwf

10. Офіційний сайт Cisco. [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/uk_ua/index.html

11. Official website Grandstream.[Online]. Available: https://www.grandstream.com/

12. Official website MikroTik.[Online]. Available: https://mikrotik.com/

13. Official website Juniper.[Online]. Available: https://www.juniper.net/

14. Official website Ubiquiti. [Online]. Available: https://uisp.com/us/uisp-overview

15. О. Тарасенко, В. Христоєв, Д. Аксинін Адміністрування та моніторинг комп'ютерних мереж як метод вирішення сучасних проблем у фінансових системах. / Фінансово-кредитні системи: перспективи розвитку, 2021. № 3, С. 64-71. https://doi.org/10.26565/2786-4995-2021-3-07

16. Технології моніторингу та трафік-інжинірингу в телекомунікаційних мережах [**Електронний ресурс**] **: підручник для студ. спеціальності 172 «Телекомунікації та радіотехніка» / П. В. Кучернюк. КПІ ім. Ігоря Сікорського, 2021. 257 с. Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/cb5f54ef-a510-46f7-adbb-b5b3b28016a6/content**

17. Official website Zabbix. [Online]. Available: https://www.zabbix.com/

18. Official website Nagios. [Online]. https://www.nagios.com/.

19. Nagios Resource Library. [Online]. Available: https://library.nagios.com/

20. SoftinventivLab. [Електронний ресурс]. Режим доступу: https://www.softinventive.com.ua/best-network-monitoring-tools

21. Official website PRTG. [Online]. Available:https://www.paessler.com/prtg

22. Official website Cacti. [Електронний ресурс]. https://cacti.net/

23. Official website Observium. https://www.observium.org/

24. Official website Prometheus. https://prometheus.io/

25. Official website Kismet. https://www.kismetwireless.net/docs/readme/intro/kismet/

26. Kismet: Wi-Fi, Bluetooth, RF, and more. https://www.kismetwireless.net/

REFERENCES:

1. “Strateghija rozvytku sfery elektronnykh komunikacij Ukrajiny na period do 2030 roku. Ministerstvo cyfrovoji transformaciji Ukrajiny” [Strategy for the Development of the Electronic Communications Sector of Ukraine for the Period Until 2030. Ministry of Digital Transformation of Ukraine.] https://thedigital.gov.ua/storage/uploads/files/Стратегія:15:05.pdf
2. M.Gh. Trenjov and A.Gh. Prokopenko (2025), “Osnovni pryncypy roboty ta vymoghy do stvorennja struktur perspektyvnykh system monitorynghu rozpodilenykh informacijno-telekomunikacijnykh merezh” [Basic principles of operation and requirements for creating structures of promising monitoring systems for distributed information and telecommunication networks], Telecommunications and information technologies, № 3(84), pp.77-85. https://doi.org/10.31673/2412-4338.2024.037785
3. “Kontrolj jakosti elektronnykh komunikacijnykh poslugh. Tekhnologhiji ta procedury.” [Quality control of electronic communication services. Technologies and procedures.], Ukrainian State Center for Radio Frequencies. https://www.ucrf.gov.ua/pres-centr/news/kontrol-iakosti-elektronnykh-komunikatsiinykh-posluh-tekhnolohii-ta-protsedury
4. “Suchasnyj stan, problemy i perspektyvy rozvytku v Ukrajini elektronnykh administratyvnykh poslugh Analitychna zapyska.” [Current status, problems and prospects for the development of electronic administrative services in Ukraine. Analytical note.], Institute for Strategic Studies. https://www.niss.gov.ua/doslidzhennya/politika/suchasniy-stan-problemi-i-perspektivi-rozvitku-v-ukraini-elektronnikh
5. P.Ju. Patalashko, N.I. Kushnirenko, N.Gh. Kozachenko and N.V. Bojko (2024) “Rozrobka systemy monitorynghu podij informacijnoji bezpeky” [Development of an information security event monitoring system], Informatics and Mathematical Methods in Simulation, Vol.14, No. 4, pp. 273-283. https://DOI 10.15276/imms.v13.no3-4.282
6. I.V. Kasovsjka, O.D. Shapovalenko and I.M. Lucenko (2021) “Proghramni kompleksy merezhevogho monitorynghu dlja pidvyshhennja efektyvnosti zakhystu merezh” [Network monitoring software packages to improve network protection efficiency], Modern information protection, №1(45), pp. 47-52. https://DOI: 10.31673/2409-7292.2021.014757
7. Jakub Svoboda, Ibrahim Ghafir and Vaclav Prenosil (2015) Network Monitoring Approaches: An Overview / *International Journal of Advances in Computer Networks and Its Security*, Vol.5, issue 2, pp. 88-93. https://www.researchgate.net/profile/Ibrahim_Ghafir/publication/305957483_Network_Monitoring_Approaches_An_Overview/links/57a75c9d08aefe6167bc1f91/Network-Monitoring-Approaches-An-Overview.pdf
8. Inna Stetsenko and Anton Myroniuk (2024) Software for collecting and analyzing metrics in the highly loaded applications based on the Prometheus monitoring system / *Information, Computing and Intelligent Systems*, № 5, pp. 17–28. https://doi.org/10.20535/2786-8729.5.2024.316366
9. Atish Barhate Comparison of Network Monitoring Tools: PRTG, SolarWinds, Nagios, Zabbix, and Datadog. https://www.linkedin.com/pulse/comparison-network-monitoring-tools-prtg-solarwinds-nagios-atish-b-26bwf
10. *Official website* сайт Cisco. https://www.cisco.com/c/uk_ua/index.html
11. *Official website Grandstream.*[Online]. Available: https://www.grandstream.com/
12. *Official website MikroTik.*[Online]. Available: https://mikrotik.com/
13. *Official website Juniper.*[Online]. Available: https://www.juniper.net/
14. *Official website Ubiquiti*. [Online]. Available: https://uisp.com/us/uisp-overview
15. O. Tarasenko, V. Khrystoiev and D. Aksynin (2021)“Administruvannia ta monitorynh kompiuternykh merezh yak metod vyrishennia suchasnykh problem u finansovykh systemakh” [Administration and monitoring of computer networks as a method of solving modern problems in financial systems] Financial and credit systems: development prospects, № 3, pp. 64-71. https://doi.org/10.26565/2786-4995-2021-3-07
16. P. V. Kucherniuk (2021)“Tekhnolohii monitorynhu ta trafik-inzhynirynhu v telekomunikatsiinykh merezhakh” [Monitoring and traffic engineering technologies in telecommunication networks] 257 p. https://ela.kpi.ua/server/api/core/bitstreams/cb5f54ef-a510-46f7-adbb-b5b3b28016a6/content
17. *Official website Zabbix*. [Online]. Available: https://www.zabbix.com/
18. *Official website Nagios.* [Online]. https://www.nagios.com/.

19. *Nagios Resource Library*. [Online]. Available: https://library.nagios.com/
20. *SoftinventivLab*. https://www.softinventive.com.ua/best-network-monitoring-tools
21. *Official website PRTG*. https://www.paessler.com/prtg
22. *Official website Cacti*. https://cacti.net/
23. *Official website Observium*. https://www.observium.org/
24. *Official website Prometheus.* https://prometheus.io/
25. *Official website Kismet*. https://www.kismetwireless.net/docs/readme/intro/kismet/
26. *Kismet: Wi-Fi, Bluetooth, RF, and more*. https://www.kismetwireless.net/

Ph.D. Pogrebniak L.M., Lukina K.V.

ANALYSIS OF MONITORING MEANS OF ELECTRONIC COMMUNICATION NETWORKS

The article considers current issues of monitoring electronic communication networks in the context of the rapid development of information technologies, the growth of cyber threats, and the peculiarities of the functioning of network infrastructure during martial law.

The main attention is paid to the analysis of modern software and hardware tools used to monitor the performance and security of electronic communication networks, as well as for the prompt detection of overloads, failures, anomalies, and potentially dangerous activity.

A comparative analysis of modern network monitoring tools from leading communication equipment manufacturers, including Cisco, MikroTik, Juniper, Ubiquiti and Grandstream, was conducted. It was shown that the tools they offer provide effective functionality, automated updates, flexible data analysis tools, and support, but have limited integration capabilities with devices from other manufacturers. This makes it difficult to implement centralized monitoring systems in networks with a mixed structure.

Independent universal monitoring systems, such as Zabbix, Nagios, NeDi, PRTG Network Monitor, Cacti, Wireshark, which are able to interact with a wide range of different types of network equipment using open protocols (SNMP, HTTP/HTTPS API, ICMP), are also considered. The advantages of such systems in the context of scalability, adaptability and configuration flexibility are shown.

The feasibility of a hybrid approach to building monitoring systems is substantiated, which combines the functionality of vendor and independent solutions, which allows achieving a high level of data detail and visualization, performing operational analytics in real time, forming an effective incident response system, and ensuring high resilience of a heterogeneous network to external influences and cyber threats.

Keywords: monitoring, monitoring tools and systems, network management, services, network resources, security.