УДК 621.39+004
DOI: 10.31673/2412-9070.2024.063392
А. Г. ПРОКОПЕНКО, аспірант;
ORCID 0009-0009-7227-3458
М. Г. ТРЕНЬОВ, асистент,
ORCID 0009-0002-8459-0599
Державний університет інформаційно-комунікаційних технологій, Київ

АНАЛІЗ НОВИХ ТЕХНОЛОГІЙ І ПЕРСПЕКТИВ РОЗВИТКУ ТЕХНІКИ ЗАСОБІВ ЗВ'ЯЗКУ

Стаття розглядає загальні вимоги і підходи до побудови перспективних систем мережевого моніторингу на основі аналізу діючих технологій та існуючих систем моніторингу інформаційно-телекомунікаційних мереж загального користування.

Метою роботи є проведення огляду існуючих систем моніторингу та вироблення нових загальних принципів і вимог до побудови мережевих моніторингових систем нового покоління. Це включає розробку архітектурних підходів і визначення критеріїв ефективності для забезпечення більшої стійкості та адаптивності таких систем.

Використані в дослідженні методи включають методи системного аналізу, що дозволяють комплексно оцінити технічний стан мереж, а також системне проєктування, яке допомагає формувати архітектуру нових рішень. Застосовуються також сучасні технології мережевого моніторингу, серед яких виділяються Site/System Reliability Engineering (SRE) — підхід, що спрямований на підвищення надійності та стабільності систем, і Operation Support Systems (OSS) — системи підтримки операцій, які забезпечують контроль і управління мережею. Ці технології допомагають удосконалити управління мережею, забезпечуючи своєчасну діагностику, прогнозування проблем та ефективне реагування на відмови.

В статті для підвищення стійкості і надійності підконтрольної мережі ключовим архітектурним принципом проєктування сучасних підсистем моніторингу гетерогенних інформаційно-телекомунікаційних мереж обрано принцип розподіленості та децентралізації.

В роботі визначено функції підсистеми мережевого моніторингу і сервера моніторингу, як ключового її елементу. Запропоновано варіант структури сервера моніторингу. Розглянуто об'єкти моніторингу, що призначаються, а також перелік зібраних з них метричних даних з точки зору функціональної продуктивності мережі. Сформульовано загальні вимоги до перспективних систем мережевого моніторингу, а також загальні принципи організації і функціонування підсистем моніторингу інформаційно-телекомунікаційної мережі.

Ключові слова: інформаційно-телекомунікаційна мережа, сервер моніторингу технічний стан, підсистема мережевого моніторингу, децентралізація моніторингу.

Вступ

Розвиток інформаційних технологій (ІТ) протягом останніх десятиліть призвів до істотних змін в загальних підходах до побудови і вдосконалення інфокомунікаційних мереж (ІКМ). Ключовими тенденціями при цьому залишаються процеси інтеграції мереж зв'язку з комп'ютерними мережами та поява розподілених гетерогенних ІКМ різного масштабу [1], що характеризуються широким впровадженням і застосуванням ІТ на базі концепції "Індустрія 4.0" (інтернет речей, "розумне місто", "розумний будинок" та ін.), забезпечують користувачам надання різних інфокомунікаційних послуг на основі стека протоколів TCP/IP/MPLS, з використанням мереж нового покоління GN (Next Generation Networks), ядро яких складають пакетні мережі. При цьому технічна платформа ІКМ представляється структурованою сукупністю швидкісних каналів зв'язку, вузлів комутації, серверів послуг і сервісів зв'язку, що діють в інте-

ресах користувачів ІКМ, а також ієрархічної автоматизованої системи управління зв'язком (АСУЗ). Фундаментальною вимогою для будь-якої АСУЗ гетерогенною ІКМ є ефективний моніторинг її ресурсів, при якому потрібні точні і актуальні оновлення в інтересах підтримки своєчасної реконфігурації мережі (управління мережевими ресурсами) з метою усунення передвідмовного її стану і недопущення аварії.

Підтримка на високому рівні ефективності функціонування ІКМ загального користування (ЗК) упродовж своїх етапів життєвого циклу (ЖЦ) безпосередньо залежать від значень показників поточної функціональної надійності її мережевих елементів і сегментів. Наслідки виникнення відмов або дефектів в ІКМ, обслуговуючих галузі з критично важливих інфраструктур (КВІ), можуть привести до глобальних катастроф з фінансовим збитком. У зв'язку з чим, на сьогодні в телекомунікаційній галузі активно ведеться розробка нових технологій підтримки функціональної безпеки ІКМ і систем, спрямованих на забезпечення їх експлуатаційної надійності, а питанням проведення заходів по діагностиці і моніторингу технічного стану (контролю) приділяється значна увага. Наприклад, на впровадження методів неруйнівного контролю на експлуатаційних етапах ЖЦ атомної електростанції витрати можуть складати до 50 % експлуатаційних витрат. Категоричність сучасних екологічних нормативів і вимог громадськості про необхідність виключення техногенних аварій і катастроф з людськими жертвами і величезним збитком для довкілля робить проблему підтримки надійності і функціональної безпеки ІКМ актуальною, а розробку систем моніторингу функціонального стану їх елементів – пріоритетною.

Під моніторингом технічного стану (ТС) мається на увазі складова частина технічного обслуговування, що полягає в спостереженні за об'єктом з метою отримання інформації про його ТС і робочі параметри. На основі даних моніторингу здійснюється контроль технічного стану або залишкового ресурсу об'єкта контролю.

Моніторинг в інформаційно-телекомунікаційній галузі, в невеликій компанії або в центрі обробки даних (ЦОД), потрібний для того, щоб системні адміністратори ІКМ були оповіщені раніше або хоча б одночасно з користувачами про відмови і проблеми в мережевій інфраструктурі. Необхідність прогнозу, а тим самим і запобігання відмов, своєчасне сповіщення про них і зберігання інформації про ТС ІКМ і її мережевих елементів забезпечує актуальність цієї роботи. Моніторинг - це комплекс швидкого знаходження проблеми, сповіщення про неї адміністраторів мережі, а також діагностики, що дає повну і точну інформацію про відмову об'єктів контролю (ОК) ІКМ.

Особливості сучасних ІКМ при побудові їх підсистем моніторингу

Одним з мало досліджених і ще невирішених завдань є побудова підсистеми моніторингу процесів функціонування територіально розподілених систем різної складності. При цьому, сучасні ІКМ як загального користування (ЗК), так і спеціального призначення (СП) можна цілком віднести до гетерогенних мереж, що також накладає певні труднощі і особливості побудови їх підсистем моніторингу. Гетерогенність (неоднорідність) мережі припускає несумісність вузлів, що належать одній мережі, або до суміжних сегментів мережі за одним або декількома логічними ознаками: за типом вживаних операційних систем, форматами кадрів мережі, моделями безпеки, способами захисту інформації і ін. З чого виходить, що в гетерогенних ІКМ підсистема моніторингу повинна будуватися на основі принципу децентралізації і багаторівневості. При тому, що ІКМ, як правило, має строго ієрархічну структуру, її підсистема моніторингу повинна дозволяти здійснення перерозподілу функцій центру управління функціонуванням і периферією залежно від поточного стану.

Складність і актуальність створення підсистем моніторингу для таких гетерогенних ІКМ зв'язано разом з їх особливостей ще і рядом обмежень, серед яких можна виділити наступні: наявність різнорідних протоколів взаємодії між вузлами і периферійними мережевими пристроями, постійні трансформації мережевих типологій і структур мережі, сполучення сегментів малопотужних і високопродуктивних елементів мережі, широке застосування мобільних станцій і пристроїв з низьким енергоспоживанням, слабкою обчислювальною потужністю,

малим об'ємом пам'яті). Вказані особливості ІКМ дозволяють вести мову про недосконаліть існуючих систем контролю, орієнтованих на застосування в гомогенних мережевих структурах і необхідності пошуку нових технологій і підходів до побудови систем розподіленого моніторингу функціонального стану сучасних гетерогенних мереж зв'язку, включаючи методи інтелектуального моніторингу.

Аналіз діючих систем мережевого моніторингу

Проаналізуємо деякі підсистеми мережевого моніторингу.

System Center Operations Manager (SCOM) - система наскрізного моніторингу (від Microsoft) і активного спостереження за будь-якими мережевими пристроями, що підтримують протокол обміну інформацією SNMP (до рівня порту), виявлення віртуальних локальних обчислювальних мереж (VLAN) і комутаторів в них, стеження за їхніми ТС.

Одним з головних переваг SCOM є просунута візуалізація усього зібраного набору метрик і представлення їх у вигляді графіків і діаграм. При цьому візуалізація доступна як в спеціальній консолі програми, так і через вебінтерфейс.

Проте SCOM має і ряд недоліків з точки зору рішення свого функціонала: вона охоплює безліч загальних показників системи, але непридатна для стеження за специфічними параметрами; досі робота з ОС поза сімейством Windows нестабільна; вимагає установки сервісу агента; істотна громіздкість і трудомісткість налаштування "під себе": система більше підходить для моніторингу загального стану і збору основних відомостей про глобальну структуру (безлічі клієнтських і серверних машин в домені). Також до недоліку системи можна віднести високу вартість цього програмного продукту.

Zabbix [2] - вільно поширювана система для проведення комплексного моніторингу мережевого устаткування, серверів і сервісів.

За допомогою Zabbix зазвичай здійснюють розподілений моніторинг до 1000 вузлів, де конфігурація молодших вузлів в ієрархії контролюється старшими. Також продукт включає централізований моніторинг лог-файлів. При цьому є можливість створювати вручну за шаблоном карти мереж, виконувати запити в різні БД, генерувати звіти і виявляти тенденції зміни метрик, виконувати сценарії на основі результатів моніторингу, підтримувати інтелектуальний інтерфейс управління платформами (IPMI).

Zabbix дозволяє здійснювати: автоматичне виявлення IP- адрес по діапазону, доступні сервіси і робити SNMP перевірку; автоматичний моніторинг виявлених мережевих пристроїв, а також автоматичне видалення відсутніх хостів; розподіл по шаблонах і групах залежно від отриманого результату та ін.

Серед недоліків варто зазначити: громіздкість сервісу, відсутність повної документованості можливостей і необхідність установки агентів на всі машини, а також складність делегування прав. Так, машина з сервісом часто керується ОС сімейством *nix, що робить працемісткою взаємодію з доменними користувачами і правами з Active Directory (Windows).

Nagios [3] - вільно поширюване програмне забезпечення (ПЗ) під моніторинг ІКМ, спочатку розроблене для ОС на базі Linux, але ефективно працює під Sun Solaris, HPUX, FreeBSD, AIX. За допомогою Nagios доступні: моніторинг безпеки ІКМ, комплексний моніторинг за ІТ-інфраструктурою, можливість оповіщати адміністратора мережі про отримувані при спостереженні дані, виявлення проблем відразу після їх виникнення, що скорочує час простою і комерційні втрати.

До недоліків використання Nagios відносять "загальний" характер моніторингу і його "мережева" спрямованість, а також проблеми взаємодії з серверами під ОС Windows.

Cacti [4] - безкоштовний додаток моніторингу, який дозволяє збирати статистику по метриках за визначеними тимчасовими інтервалами з відображенням їх в графічному вигляді при використанні утиліти RRDtool, призначеної для функціонування з круговими базами даних (типу Round Robin Database) і інформації, що використовується для зберігання, про зміну одного або декількох параметрів за певний проміжок часу. Стандартно шаблон збору включає

статистику про завантаження процесора, кількість запущених процесів, використання трафіку, що входить/виходить, виділення оперативної пам'яті.

До переваг Cacti відносять: високу швидкість розгортання при мінімальному додатковому кодуванні, простоту і зручність інтерфейсу налаштування перегляду звітів.

До недоліків Cacti можна віднести: швидке наростання числа однотипних налаштувань при великій кількості середовищ і серверів; обмежена продуктивність "нерідних" JMX рішень; неможливість інвентаризації при перерозподілі ресурсів і модернізації.

Prometheus - вільно поширюване ПЗ в інтересах моніторингу мережевих пристроїв, серверів і сервісів, має вбудований базовий мережевий інтерфейс, але частіше використовується в зв'язці з сервером візуалізації даних **Grafana.** До її складу входять:

Сервер моніторингу виконує регулярне опитування, збір, обробку та аналіз даних. У разі виявлення аномалій він звертається до інтерфейсу сповіщення оператора. Завдяки цьому серверу можна віддалено контролювати роботу мережевих сервісів. Він слугує сховищем, де зберігаються конфігураційні, статистичні й оперативні дані про структуру мережі та стан її елементів. Сервер має зручний інтерфейс для доступу до даних і підтримує інтеграцію з іншими сервісами, такими як інтерфейс сповіщень чи інтерфейс відображення. Основним недоліком є те, що він не підходить для розгортання на серверах, що працюють під управлінням операційних систем Windows.

Системи підтримки операцій (OSS), створені на базі протоколів SNMP версій 1 і 2, широко застосовуються провідними телекомунікаційними компаніями. У рамках високорівневої архітектури OSS, до якої належать рішення Hewlett-Packard OpenView (HP OpenView - NNM), OpenNMS та Huawei U2000LCT, центральним елементом виступає налаштовуваний компонент диспетчеризації подій, інтегрований із класифікатором подій, відмов і попереджень відповідно до рекомендацій M.3703.

У різних OSS цей компонент реалізується по-різному: у OpenNMS це процес-диспетчер EventD, у HP OpenView — PMD, а в Huawei U2000LCT — MRB.

Функціональні сервіси OSS, підключені до диспетчера подій, реалізуються через проєкції управління, які охоплюють: управління відмовами, управління конфігураціями, облік ресурсів, управління продуктивністю та забезпечення безпеки.

Крім того, OSS містить такі важливі компоненти:

- Аналіз структури мережі (наприклад, ovtopmd у HP OpenView, discovery в OpenNMS, Discovery Service у Huawei U2000LCT);
- Збір даних і SNMP-трапів (collectd і trapd у OpenNMS, snmpcollect і ovtrapd у HP OpenView, NEDataCollector у Huawei U2000LCT);
- Тестування високорівневих сервісів (ovcapsd у HP OpenView, capsd і poller у OpenNMS);
- Обробка відмов (ovalarm у HP OpenView, outaged у OpenNMS).

Таким чином, системи OSS забезпечують комплексний підхід до моніторингу та управління мережею за допомогою модульної архітектури та спеціалізованих компонентів.

У даних OSS можна виділити 3-рівневу схему обробки: дані (date), що отримуються за допомогою вимірів; події (events), що отримуються після обробки процесами збору первинних даних при порівнянні метрики з пороговим значенням; відмови (faults) і попередження (alarms), що отримуються в результаті логічного висновку на багатьох подіях (events). У процесі обробки спостерігається скорочення об'єму даних при переході від даних до подій і від подій до відмов. Ця процедура переходу регламентується класифікатором подій, який будується на основі рекомендацій M.3703.

Події в системах управління характеризуються не лише класом, часом генерації та ідентифікатором пристрою-джерела, що діагностується, але також адресою, яка викликала подію, та ідентифікатором програмного компонента, що її створив.

Дані поля умовно поділяються на дві частини:

Об'єкт управління – це пристрій, до якого належить подія.

Суб'єкт управління – агент або програмний компонент, який виконує операції над мережевим елементом у межах системи управління (СУ).

Під час обробки подія може передаватися між суб'єктами за певною послідовністю:

1. **Пристрій** (об'єкт події).
2. **Агент** (виконує передачу даних).
3. **Компонент збору даних** (відповідає за акумуляцію інформації).
4. **Компонент діагностики** (аналізує дані та визначає аномалії).

Таким чином, обробка подій створює ієрархічні ланцюжки суб'єктів, які послідовно взаємодіють для забезпечення моніторингу та управління мережею.

Одна з технологій, яка активно завойовує ринок IT-послуг для телеком-операторів та спрямована на забезпечення експлуатаційної надійності ІКМ і систем, — це SRE (Site/System Reliability Engineering). Вона являє собою набір інженерних практик, орієнтованих на підтримку надійної та безвідмовної роботи додатків як у поточний момент, так і в майбутньому [5].

SRE спрямована на виявлення аномальних ситуацій і проблем у роботі ІКМ ще до того, як про них стане відомо користувачам. Концепція цієї технології зосереджена на вирішенні внутрішніх завдань ІКМ, зокрема вимірюванні часу безвідмовної роботи мережевих елементів і сервісів, а також точному визначенні їх доступності з урахуванням вимог до масштабованості та реакції на непередбачені обставини.

Технологія SRE передбачає усунення організаційних бар'єрів між командами, що займаються розробкою спеціалізованого ПЗ, і фахівцями з інформаційно-технологічного обслуговування. Це досягається шляхом інтеграції їхніх робочих процесів, використання спільних метрик оцінки функціональної надійності та розподілу загальної відповідальності між усіма учасниками процесу надання інформаційно-телекомунікаційних послуг на різних етапах життєвого циклу ІКМ.

Наприклад, показниками доступності в рамках підходу SRE є такі часові метрики:

SLI (Service Level Indicator) – це індикатори продуктивності, як-от пропускна здатність, затримка запитів, кількість запитів за секунду та частота збоїв на запит. Ці дані агрегуються за певний час і перетворюються в середні значення (або у відсотки) щодо встановленого порогу.

SLO (Service Level Objective) – це цільові значення метрик SLI за визначений звітний період, наприклад, добу, тиждень, місяць, квартал або рік.

При цьому важливо зазначити, що будь-які простої мережі можуть призвести до фінансових втрат для телеком-оператора. Тому необхідно забезпечувати моніторинг актуальних значень метрик SRE у режимі реального часу:

RPO (Recovery Point Objective) – це максимальний час, протягом якого можуть бути втрачені дані внаслідок інциденту. Для телеком-оператора цей показник повинен бути мінімізований, а в ідеалі – зведений до нуля (RPO → 0). Інструменти, як-от автоматична реплікація даних у файловій системі, допомагають знижувати RPO, однак цього недостатньо для забезпечення високої доступності сервісу. Визначення та оптимізація RPO належить до завдань DevOps- та SRE-інженерів.

RTO (Recovery Time Objective) – це час, протягом якого система може бути недоступною внаслідок збою чи аварії (тобто цільовий час на відновлення). Цей інтервал охоплює відновлення повної функціональності системи або сервісу. Завдання SRE-інженерів – організувати систему таким чином, щоб за допомогою технологій відмовостійкості та відновлення даних з резервних копій оперативно відновити працездатність сервісу на резервному обладнанні або майданчику. Оптимізація процесу спрямована на мінімізацію значень RPO та RTO.

Впровадження систем моніторингу в корпоративних ІКМ є особливо важливим у контексті застосування сервісного підходу в роботі IT-підрозділів. У такому підході всі процеси забезпечення функціональної надійності подаються з точки зору послуг, які надає IT-підрозділ. Кожен бізнес-сервіс корпоративної ІКМ, за можливості, трактують як IT-сервіс, який описується у системі моніторингу через набір взаємопов'язаних компонентів IT-інфраструктури із зазначенням рівня якості його надання кінцевому користувачу.

На основі такого підходу формують угоду про рівень якості сервісів (SLA – Service Level Agreement). Ця угода визначає умови, за якими система моніторингу здійснює збір і збереження даних про якість надання ІТ-сервісів. Зібрані метрики аналізуються та використовуються для формування звітів за встановлений період. Аналіз цих звітів дозволяє оцінити та коригувати рівень надання ІТ-сервісів, оптимізувати роботу ІТ-підрозділу планувати та проводити модернізацію ІТ-інфраструктури.

Одним із ключових завдань технології SRE є забезпечення і підтримка заданого рівня доступності мережевих елементів корпоративних інформаційно-комунікаційних мереж (ІКМ). Це включає визначення основних показників надійності, які підлягають постійному моніторингу, вимірюванню та оцінці. У SLA-договорах між постачальниками телекомунікаційних послуг і споживачами зазвичай фіксуються наступні контрольні метрики якості ІТ-сервісу є доступність (**availability**), продуктивність (**performance**), надійність (**reliability**), ремонтопридатність (**maintainability**), обслуговуваність (**serviceability**), безпека (**security**) [6].

Водночас SLA-договори регулюють відносини з кінцевими споживачами, тоді як технологія SRE орієнтована переважно на внутрішнє використання для взаємодії технічних служб підтримки. Зазвичай вимоги SRE до якості сервісів є суворішими, ніж ті, що зазначені в SLA-договорах.

Для ефективної взаємодії між двома ІКМ або їх сегментами зазвичай використовують вбудовані засоби контролю і управління (моніторинг OSS) у межах ореолу дії мережі та незалежні вимірювальні засоби контролю (моніторинг SLA) у точках демаркації.

Системи моніторингу SLA переважно застосовуються в точках демаркації, оскільки в інших зонах показники мережі ефективно контролюються вбудованими системами управління та самодіагностики (рівня NMS). Це дозволяє мінімізувати складність управління мережею та зосередитися на базовій функціональності системи.

Замість розгортання глобальної системи управління за підходом NMS-TMN-OSS, можна обмежитися створенням базової системи управління мережею з наступними ключовими елементами:

- об'єднання NMS між собою через угоди в SLA-договорах;
- інтеграція моніторингу SLA для покриття точок демаркації.
- Цей підхід, хоч і поступається за функціональністю більш складним інформаційним системам управління, має такі переваги:

- низька вартість рішення;
- швидкість розгортання – від 2 до 3 тижнів;
- можливість впровадження без залучення зовнішніх фахівців чи інтеграторів.

Запропонована система, являючись універсальною, підтримує різноманітне мережеве обладнання та охоплює широкі географічні території, що робить її ефективним і практичним рішенням для багатьох корпоративних ІКМ.

Хоча застосування систем моніторингу SLA обмежується точками демаркації між підмережами, це не зменшує їхньої значущості. З огляду на зростання кількості таких точок, спричинене розширенням асортименту систем, сервісів і обладнання, важливість цих засобів контролю лише зростає. Крім того, розвиток ІТ-технологій розширює область кваліметрії та метрології в точках демаркації.

Географічне обмеження сфери застосування моніторингу SLA дозволяє зосередитися на вирішенні завдань контролю якості без втручання у внутрішні системи управління OSS, сприяючи ефективнішому розподілу ресурсів.

Виділяють три основні типи точок демаркації [7] (рис. 1):

1. Оператор-оператор – точка взаємодії між операторами зв'язку.
2. Оператор-користувач – точка підключення клієнта до мережі.
3. Внутрішні точки демаркації – розташовані між виробниками, структурними підрозділами або регламентними елементами ІКМ.

Для внутрішніх точок демаркації використовується угода операційного рівня, яка встановлює правила взаємодії всередині організації.

У точках демаркації доцільно застосовувати спеціалізовані вимірювальні пристрої (метрологічні засоби), оскільки вбудовані засоби діагностики в цих точках зазвичай не працюють. Крім технічних рішень, для розв'язання конфліктних ситуацій необхідно нормувати відповідні па-раметри в рамках SLA-договорів. Це дозволяє забезпечити об'єктивність оцінки та справедливе розв'язування спірних питань. SLA забезпечує операторам можливість узгодження параметрів взаємодії, незалежно від чинних стандартів. Завдяки цьому один оператор може запропонувати транзит свого трафіку через мережу іншого оператора, гарантувавши збереження характеристик трафіку в межах допустимих значень. Наприклад, транзитна мережа не має права збільшити частку втрачених викликів більш ніж на 5% через свою діяльність.

У випадках, коли йдеться про нову технологію, для якої ще не існує національних стандартів або нормативних документів, SLA стає єдиним інструментом для регулювання взаємин між сторонами. Він дозволяє уникнути правового вакууму та встановлює чіткі правила співпраці навіть у ситуаціях, коли формальні регуляторні вимоги ще не розроблені.

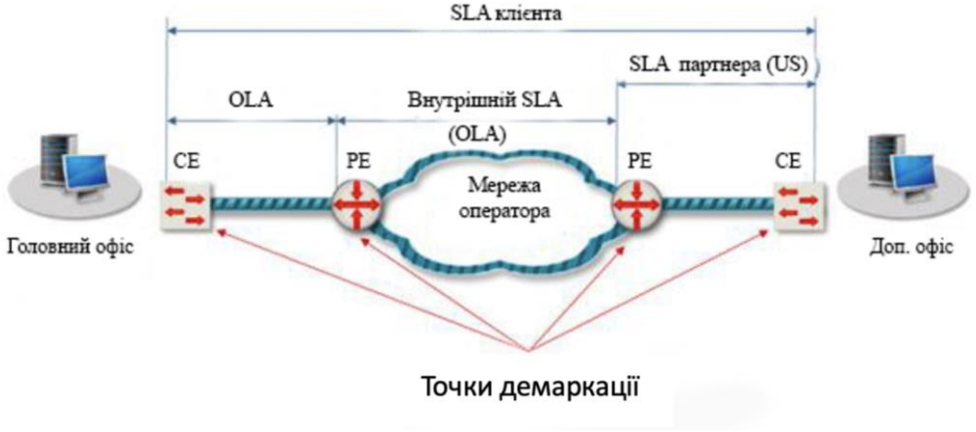

Рис. 1. Варіанти точок демаркації

Перехід від підходу «відповідність/невідповідність національним стандартам» до використання SLA сприяє підвищенню загальної якості роботи ІКМ завдяки більш жорстким вимогам. Такий підхід забезпечує гнучкість у комерційній та маркетинговій діяльності оператора, що стає важливим фактором успіху.

Сучасні системи моніторингу SLA мають процесно-орієнтовану архітектуру, яка відрізняється від традиційних систем OSS/BSS. На відміну від останніх, системи SLA інтегруються з процесами інформаційного обміну, що забезпечує їхню тісну прив'язку до специфіки телекомунікаційних послуг.

Основою функціонування систем моніторингу SLA є управління наскрізними процесами життєвого циклу послуги. Це дозволяє ефективно вирішувати конфлікти між постачальником і споживачем послуг зв'язку шляхом аналізу, контролю і вдосконалення процесів на всіх етапах надання послуги (рис. 2).

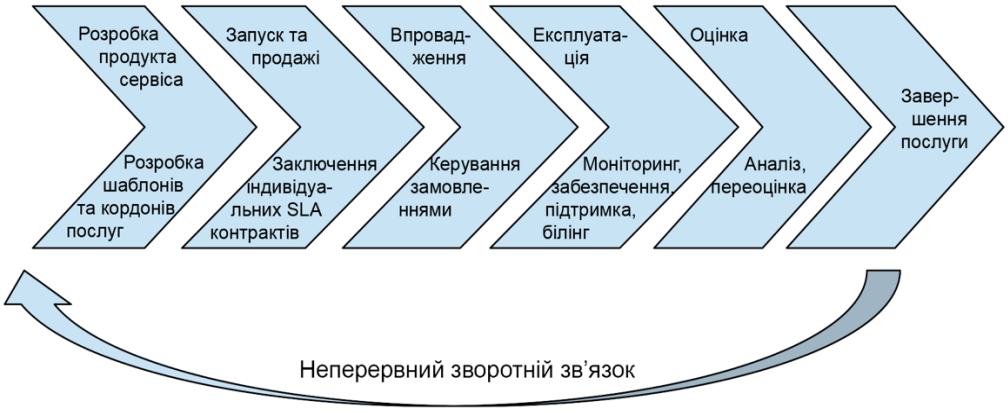

Рис. 2. Наскрізний цикл надання послуг відповідно до SLA-контракту

Система моніторингу SLA орієнтована не на управління окремими послугами чи метриками, а на повноцінне управління контрактами SLA. Це забезпечує комплексний підхід до організаційно-технічних процедур, пов'язаних з управлінням SLA, зокрема, узгодження та затвердження SLA-договорів, управління їхніми змінами та версіями та дотримання стандартів і політик якості оператора.

Такий підхід робить системи моніторингу SLA надзвичайно актуальними та важливими, відносячи їх до класу найсучасніших рішень. Їхня процесно-орієнтована структура забезпечує результативність, що разом із швидким розгортанням і високою технологічністю підсилює конкурентоспроможність цих систем на ринку IT.

На відміну від систем OSS, які активно втручаються в роботу обладнання, системи моніторингу SLA виконують лише функцію контролю, не змінюючи конфігурацію чи режими роботи мережі. Завдяки цьому вони забезпечують оперативний і повний контроль над станом як окремого сегмента мережі, так і всієї інфраструктури загалом.

До того ж SLA дозволяє враховувати індивідуальні особливості мережі або її сегментів, надаючи можливість гнучко вимірювати та оцінювати їхній стан. Це робить системи SLA універсальним і ефективним інструментом для забезпечення якості послуг у складних мережевих середовищах.

Важливо зазначити, що лише моніторинг мережі в режимі реального часу здатен надати телеком-оператору об'єктивну картину метрик SRE, які характеризують доступ споживачів до додатків ІКМ. Якщо SLA-договори спрямовані переважно на регулювання відносин із зовнішніми споживачами послуг, то метрики SRE є ключовими для внутрішніх потреб оператора. Вони дозволяють сформувати загальну відповідальність технічного персоналу та SRE-інженерів за забезпечення доступу до додатків і сервісів у межах функціонування ІКМ.

Постійний моніторинг якісних параметрів ІКМ, разом із інтегрованою системою управління, збору та обробки вимірювальної інформації (BI) у реальному часі, забезпечує об'єктивне розуміння стану функціональної безпеки мережі. Це стосується, зокрема, надання доступу до додатків, які можна умовно поділити на дві категорії:

1. Критично важливі додатки – їхня незадовільна робота може призвести до кримінальної відповідальності користувача.
2. Додатки, що залежать від якості мережевих послуг – при поганій якості можуть спричинити фінансові та репутаційні втрати для користувача.

У таких випадках SRE-метрики можуть слугувати основою для судових претензій до телеком-оператора, якщо їх якість включена до SLA-договору.

Таким чином, моніторинг мережі за метриками SRE сьогодні є найбільш об'єктивним і надійним підходом для оцінки параметрів ефективного функціонування ІКМ. Це підкреслює необхідність подальшого розвитку та вдосконалення інструментарію SRE для забезпечення високої якості послуг.

Існує широкий спектр рішень для моніторингу, що працюють як на загальнодоступних, так і на приватних хмарних платформах. Розглянемо декілька з них:

Amazon CloudWatch [8] – служба моніторингу та управління, розроблена для відстеження використання віртуальних ресурсів у хмарі Amazon, таких як екземпляри віртуальних машин **Amazon EC2**. Вона забезпечує зручний інструмент для аналізу продуктивності та доступності хмарної інфраструктури.

PCMONS [9] – система моніторингу, орієнтована на приватні хмари. Її можна адаптувати для використання постачальниками хмарної телефонії, забезпечуючи збір та централізацію інформації про використання ресурсів.

IBM Tivoli Monitoring [10] та **HP Open View** [11] – інструменти моніторингу, спрямовані на підвищення продуктивності та доступності IT-інфраструктур. Вони зосереджуються переважно на фізичних ресурсах, надаючи аналітичні дані для оптимізації їх використання.

MonPaaS [12] – адаптивна платформа моніторингу з відкритим вихідним кодом, що функціонує за принципом "моніторинг як послуга". Вона інтегрує можливості Nagios та OpenStack для відстеження фізичних і віртуальних ресурсів, а також автоматично оновлює інформацію

про зміни у фізичній чи віртуальній інфраструктурі. Основний недолік MonPaaS – додаткове споживання фізичних ресурсів.

Ці рішення дозволяють адаптувати процес моніторингу до специфіки хмарних середовищ, забезпечуючи ефективний контроль за використанням ресурсів та їх оптимізацією.

Висновки

У статті подано огляд працюючих технологій та систем мережевого моніторингу ІКМ ЗК. Дана характеристика таких як SCOM, Zabbix, Nagios, Cacti, OSS, SRE, SLA, Amazon CloudWatch, IBM Tivoli Monitoring, GMonE, PCMONS та інших. Їх огляд показав, що у міжвідомчих розподілених ІКМ обчислювальні потужності на межах мережі зростають, а хмарні обчислення, які традиційно забезпечуються наданням інфраструктурних послуг у великих ЦОД, переміщуються на кордон мережі. Причому зростання доступності периферійних інфраструктур також підштовхує додатки, які працюють у віддалених ЦОДах, до роботи на розподілених периферійних пристроях. У умовах значно змінюються загальні підходи та методи побудови перспективних підсистем моніторингу мережі.

У роботі визначено функції підсистеми мережевого моніторингу ІКМ та сервера моніторингу як ключового її елемента. Запропоновано варіант структури сервера моніторингу ІКМ та залежних підсистем. Розглянуто призначені об'єкти моніторингу, а також перелік метричних даних, що збираються з них, з точки зору функціональної продуктивності ІКМ. Сформульовано загальні вимоги до перспективних систем мережного моніторингу, а також загальні засади організації та функціонування підсистем моніторингу ІКМ. При цьому для підвищення стійкості та надійності підконтрольної мережі ключовим архітектурним принципом проєктування сучасних підсистем моніторингу розподілених гетерогенних ІКМ визначено принцип розподілу та децентралізації.

Список літератури

1. Інтеграція інформаційних ресурсів - стратегічний напрям забезпечення інформаційних потреб суспільства / І. Курас // Бібліотечний вісник. - 2004. - № 6. - С. 50-52

2. Zabbix, URL: https://www.zabbix.com/network_monitoring

3. Nagios, URL:https://www.nagios.com/nagios2024/

4. Cacti, URL:https://www.cacti.net/info/cacti

5. Operational Support System (OSS), URL: https://www.spiceworks.com/tech/networking/articles/what-is-oss/

6. Site Reliability Engineering (SRE), URL: https://aws.amazon.com/what-is/sre/

7. Базові метрики, URL: https://qagroup.com.ua/publications/what-is-metrics/

8. Basic interactions between the network, operator company and customer, URL: https://www.researchgate.net/figure/Basic-interactions-between-the-network-operator-company-and-customer-and-the_fig1_220956443

9. Amazon CloudWatch URL: https://aws.amazon.com/cloudwatch/

10. Chaves, Shirlei & Uriarte, Rafael Brundo & Westphall, Carlos. (2011). Toward an Architecture for Monitoring Private Clouds (Slides). Slides of paper published at IEEE ComMag on Dec. 2011.

11. IBM Tivoli Monitoring URL: https://www.ibm.com/docs/en/tivoli-monitoring/6.3.0?topic=introduction-overview-tivoli-monitoring

12. HP Open View URL:https://tzi.com.ua/hp-open-view.html

13. MonPaaS: An Adaptive Monitoring Platformas a Service for Cloud Computing Infrastructures and // Jose M. Alcaraz Calero; Juan Gutierrez Aguado, Services IEEE Transactions on Services Computing (Volume: 8, Issue: 1, Jan.-Feb. 2015), pp 65-78

A. Prokopenko, M. Treniov

ANALYSIS OF NEW TECHNOLOGIES AND DEVELOPMENT PROSPECTS COMMUNICATION TECHNOLOGIES

The article considers the general requirements and approaches to building advanced network monitoring systems based on the analysis of existing technologies and existing monitoring systems for public information and telecommunication networks.

The purpose of the work is to review existing monitoring systems and develop new general principles and requirements for building new generation network monitoring systems. This includes developing architectural approaches and defining performance criteria to ensure greater resilience and adaptability of such systems.

The methods used in the study include system analysis methods that allow for a comprehensive assessment of the technical condition of networks, as well as system design, which helps to shape the architecture of new solutions. Modern network monitoring technologies are also used, including Site/System Reliability Engineering (SRE), an approach aimed at improving the reliability and stability of systems, and Operation Support Systems (OSS), which provide control and management of the network. These technologies help to improve network management by providing timely diagnostics, problem prediction, and effective response to failures.

In this article, to increase the stability and reliability of the monitored network, the principle of distribution and decentralisation is chosen as the key architectural principle of designing modern subsystems for monitoring heterogeneous information and telecommunication networks.

The paper defines the functions of the network monitoring subsystem and the monitoring server as its key element. A variant of the monitoring server structure is proposed. The assigned monitoring objects are considered, as well as the list of metric data collected from them in terms of functional network performance. The general requirements for advanced network monitoring systems are formulated, as well as the general principles of organisation and functioning of information and telecommunication network monitoring subsystems.

Keywords: information and telecommunication network, technical condition monitoring server, network monitoring subsystem, monitoring decentralisation.