

УДК 621.39 (045)

DOI: 10.18372/2310-5461.38.12837

Р. С. Одарченко, канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0002-7130-1375
e-mail: odarchenko.r.s@ukr.net

А. Ю. Коберник
Національний авіаційний університет
https://orcid.org/0000-0001-7833-1879
e-mail: kobernika97@gmail.com

Т. В. Федюра
Національний авіаційний університет
orcid.org/0000-0001-5330-0822
e-mail: tanyafediura@gmail.com

ДОСЛІДЖЕННЯ АРХІТЕКТУРИ СУЧАСНИХ СИСТЕМ МОНІТОРИНГУ В МЕРЕЖАХ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

Вступ

Технологічний розвиток засобів передачі даних об'єктивно сприяє розвитку телекомунікаційної інфраструктури інформаційного забезпечення. Паралельно з цим зростає і суспільний попит на обмін інформаційними потоками на більш високому рівні. В результаті два фактори доповнюють один одного, що і зумовлює інтенсивне просування телекомунікаційних технологій у сучасному суспільстві. Безумовно, дане явище є позитивним з погляду територіального поширення та доступності телекомунікаційних послуг та поширення їх спектру. Телекомунікаційні системи у міру розвитку стикаються з проблемами, які стримують прогрес. Це пов'язано із забезпеченням безпеки, та з зростаючими цінами, оскільки більш досконалі стандарти неминуче потребують підключення великих ресурсів. Якщо ж казати про загальні тенденції, то нові телекомунікаційні технології тяжіють до принципів відкритості та загальнодоступності.

Розробники систем цілком логічно зацікавлені в більшому охопленні абонентів, що вимагає розширення інфраструктури. Відповідно, виникає проблема поєднання декількох стандартів обладнання певної якості — від бюджетного до преміального рівня. Ці та інші проблеми розвитку передбачають різні підходи в плані рішення, тому перспектива подальшого прогресу очевидна — питання лише у формах його реалізації. Внаслідок постійного розширення телекомунікаційних мереж суб'єктивно збільшується кількість сегментів, з яких складаються мережі зв'язку та телекомунікацій. Виходячи з доцільності та умов експлуатації, зазначені сегменти мають різні технології передачі даних і сигналізації.

Наприклад, при доставлянні телефонного сигналу в рамках однієї мережі можуть використовуватися ділянки, де з'єднання відбуваються як за принципом комутації каналів, так і за принципом комутації пакетів. Для забезпечення таких умов необхідно здійснити ряд організаційно-технічних заходів, одним з базових елементів яких варто передбачити впровадження комплексної системи моніторингу телекомунікаційної мережі. Створення і функціонування даної системи повинно спиратися на техніко-економічні переваги і додаткові можливості, які повинні бути отримані під час впровадження системи.

Характерними особливостями і вимогами до архітектури комплексної системи моніторингу телекомунікаційної мережі є її відкритість, модульність і доступність [1]. Відкритість забезпечує можливість використання системи комплексного моніторингу у будь-якому оточенні, зокрема, на різних апаратних платформах технічних засобів. Модульність забезпечує широкий спектр застосувань залежно від потреб кінцевого споживача, не враховуючи базову версію платформи. Стабільні інтерфейси забезпечують взаємодію декількох прикладних систем (модулів) на єдиній платформі. Доступність забезпечує кінцевому споживачеві можливість відповідно з потребами розвитку мережі (тобто, збільшення кількості елементів мережі) доповнювати систему комплексного моніторингу, витрачаючи на це мінімальні кошти.

Зібрані системою моніторингу дані можуть зберігатися у віддалених модулях [1] або негайно пересилатися в базу даних центру спостереження. Перед передачею можлива фільтрація і попередня обробка їх в віддаленому модулі, що знижує час передачі інформації до центральної бази

даних. Зібрана з усіх віддалених модулів інформація архівується в базі даних і потім може бути згрупована і статистично оброблена відповідно до запитів оператора системи (за часом спостереження, маршрутами, групам абонентів, послуг, вузлів і т. д.).

Система комплексного моніторингу має гнучку ієрархічну структуру з можливістю нарощування кожного ієрархічного рівня. До самій системі комплексного моніторингу мають бути застосовані такі принципи:

1) управління конфігурацією і роботою має здійснюватися з єдиного центру;

2) дані від територіально рознесених елементів надходять до центру по виділеній підмережі передачі даних;

3) система здійснює самоконтроль, тобто, візуалізацію і контроль функціонування всіх елементів.

З метою зменшення витрат на моніторинг телекомунікаційної мережі доцільно створити єдину мережу комплексного моніторингу телекомунікаційної мережі, яка дозволить об'єднати декілька різних мереж в одну, використавши при цьому єдиний базовий модуль збору інформації з різних програмним забезпеченням і з єдиним центром обробки інформації про стан мережі.

Аналіз досліджень та публікацій

Питанням, пов'язаним із створенням систем моніторингу сучасних телекомунікаційних мереж присвячені праці багатьох вітчизняних та закордонних учених.

У праці [1] визначені основні задачі та підстави для розгляду питань створення комплексної системи моніторингу телекомунікаційних систем, у праці [3] наведено детальну інформацію про систему розподіленого моніторингу мереж зв'язку «СПАЙДЕР». На ресурсі [4] представлена інформація, щодо одного з сучасних варіантів моніторингу мережі.

Постановка мети дослідження

Проте слід відзначити, що майже кожній системі моніторингу, розглянутій у різноманітних джерелах, притаманні свої певні риси.

У розглянутих вище працях не було приділено значної уваги системам підтримки операційної діяльності — OSS.

Метою даної роботи є дослідження систем підтримки операційної діяльності, та рішень, що наразі використовуються в телекомунікаційній індустрії для моніторингу та усунення аварійних ситуацій на мережі, а також дослідження одного з варіантів централізованої системи моніторингу мережі, що зараз існує.

Системи підтримки операційної діяльності — OSS

Операційна система підтримки (OSS — Operations Support Systems) — це набір програм, які допомагають постачальнику послуг зв'язку контролювати, аналізувати та управляти комп'ютерною мережею і забезпечувати задану якість послуг для своїх абонентів [6]. OSS-рішення дозволяють підвищити ефективність операційних процесів планування, будівництва і експлуатації мережі операторів зв'язку, виконувати інженерам свою роботу швидше, ефективніше, якісніше:

- підвищення ефективності операційних процесів — забезпечення автоматизованого інформаційного обміну в реальному масштабі часу між інженерами, які виконують взаємозалежні операції і процеси;

- підвищення ефективності роботи інженерів (центру управління, польових, субпідрядників);

- підвищення доходу за рахунок скорочення часу недоступності мережі;

- надання актуальної та достовірної інформації про кабельну, фізичну, логічну, сервісну топології мережі для інженерів, які планують, будують, експлуатують мережу;

- скорочення капітальних витрат за рахунок більш ефективного використання існуючих ресурсів мережі [5].

У табл. 1 виділені основні розбіжності між компаніями, що використовують розрізнені засоби моніторингу і тими, що використовують системи підтримки операційної діяльності. Надалі розглянуто, як саме OSS-системи вирішують недоліки розрізнених систем моніторингу.

На схемі рис. 1 показано приклад інтеграції OSS-систем для інформаційного обміну, для автоматизації завдань експлуатації мережі [5].

Проблему повільного реагування на інциденти та виділення пріоритетних аварій вирішує IBM Netcool — управління несправностями (Fault Management). Централізована система моніторингу (Umbrella Fault Management), яка дозволяє автоматизувати збирання і обробку подій для своєчасного реагування на аварії, які впливають на функціонування телекомунікаційної мережі, а також попереджувального усунення несправностей до того, як вони можуть вплинути на якість послуг.

xMatters — оповіщення про події на мережі кого це стосується, коли це потрібно і як це потрібно (Alert Management).

AmdocsCramer OSS — автоматизація процесів інвентаризації та планування мережевих ресурсів, а також експлуатації мережі (Network Inventory).

Таблиця 1

Розбіжності між компаніями, що використовують розрізнені засоби моніторингу і OSS

	Компанії, що використовують розрізнені засоби моніторингу	Компанії, що використовують системи підтримки операційної діяльності
Час обробки інцидентів	Повільне реагування (-)	Швидке реагування (+)
Виділення пріоритетних інцидентів	Відсутнє, інженери повинні самостійно виділяти найбільш загрозливі інциденти (-)	Присутнє (+)
Контроль доступу на площадки з базовими станціями	Відсутній, можна побачити проникнення на об'єкт, але немає інформації про те легальний це доступ, чи робота зловмисників (-)	Присутній, доступ на площадки з базовими станціями здійснюється відповідно до номеру заявки на роботи та ідентифікатором співробітника (+)
Автоматичний пошук кореневої причини несправності	Відсутній (-)	Присутній (+)
Автоматизація рутинних процесів та створення заявок на усунення несправності	Відсутня (-)	Присутня (+)
Інтерфейс користувача	Немає повної картини ситуації на мережі (-)	Зрозумілий інтерфейс, що дозволяє бачити повну картину ситуації на мережі (+)
Затримки надходження інцидентів	Присутні, але менші ніж у централізованих систем моніторингу, аварії відразу приходять в систему (+/-)	Присутні, адже аварії спочатку приходять у розрізнені системи і лише потім у централізовану систему моніторингу (-/+)

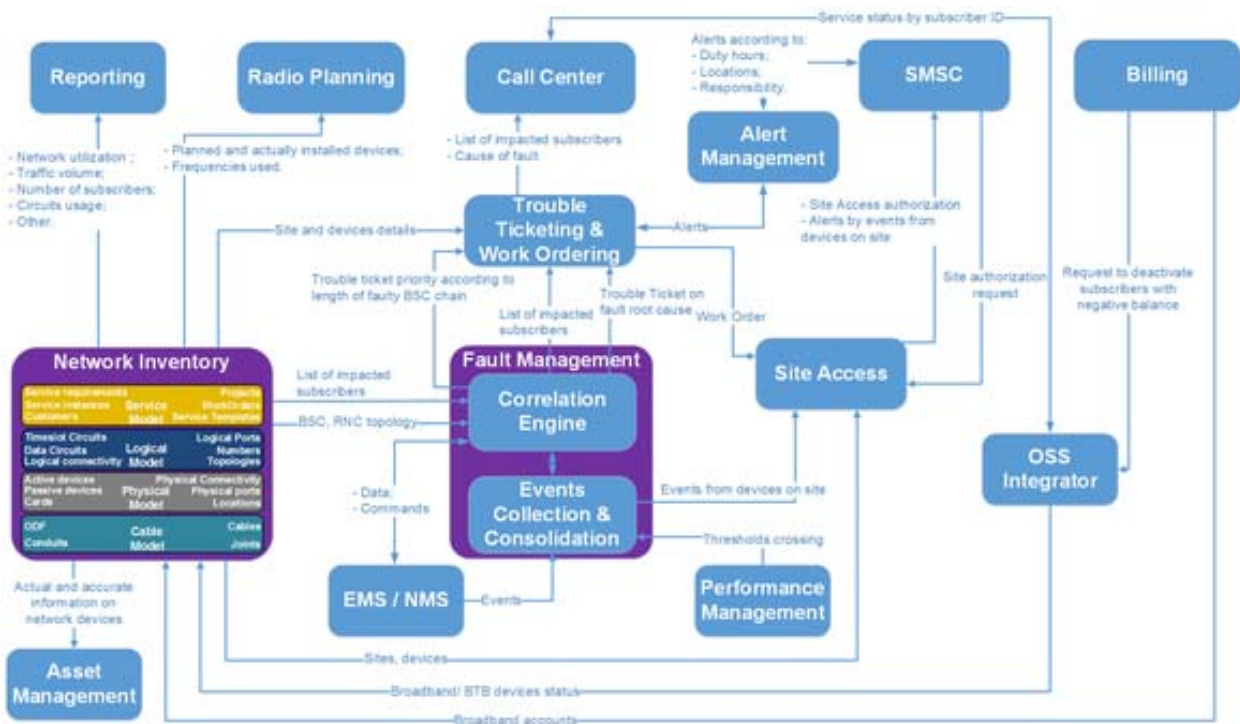


Рис. 1. Приклад інтеграції OSS-систем для автоматизації завдань експлуатації мережі

На жаль, більшість промислових програмних продуктів неможливо впровадити без додаткових зусиль по доопрацювання і конфігурації (*outofthebox*). Кожен проект є унікальним, тому що необхідна ретельна адаптація рішень до конкретних експлуатаційних моделей і процесів операторів. Крім того, зазвичай доводиться розробляти додаткові спеціалізовані додатки для забезпечення цілісності автоматизації процесів.

Site Access — рішення для автоматизації процесу контролю доступу на площадки з базовими станціями відповідно до номеру заявки на роботи і ідентифікатором співробітника, а також отримання всієї необхідної інформації про обладнання, що знаходиться на майданчику, безпосередньо на телефон інженера.

Автоматичний пошук кореневої причини несправності (Root Cause Analysis), вирішує Correlation Engine — спеціалізована платформа

для реалізації різних алгоритмів кореляції, аналізу впливу на сервіси (Services Impact Analysis) і відновлення сервісів (Runbook Automation).

OSS API — інтеграційна платформа для розширення функціональності взаємодії OSS-систем: підтримки абонентів, управління обладнанням, білінгу, інвентарних систем та ін.

OSS Mobile Client — додаток, яке надає інженеру на мобільний пристрій інформацію з декількох OSS систем у вигляді необхідному і достатньому для виконання конкретного завдання.

Алгоритми побудови крос-доменних з'єднань — спеціалізовані алгоритми, розроблені для побудови топології фізичних і логічних з'єднань у гетерогенних мережах (PDH, SDH, DWDM, RRL, ...), наприклад, актуальний маршрут підключення базової станції (BTS) до контролера (RNC) (рис. 2) [5].

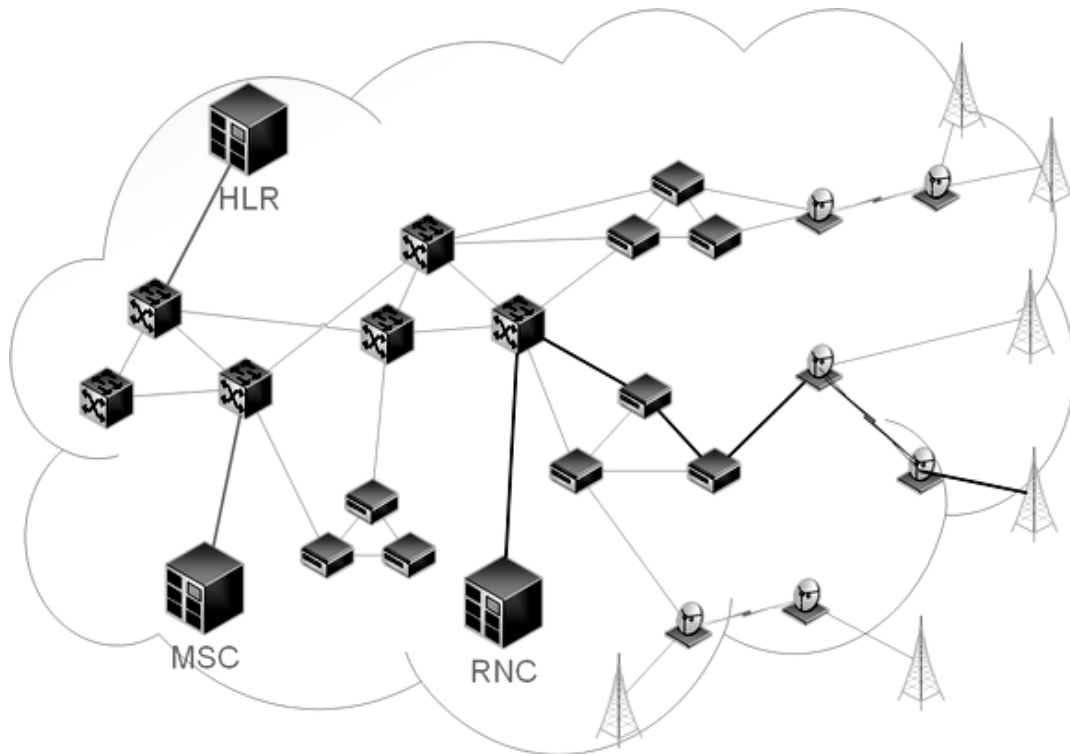


Рис. 2. Алгоритм побудови крос-доменних з'єднань

Централізоване збирання статистичної інформації від усіх об'єктів моніторингу

У компаніях і організаціях, де використовують розрізнені засоби моніторингу, відсутнє єдине уявлення про мережу, і як наслідок, про вплив тієї чи іншої події на якість надання послуг. Централізована система моніторингу дозволяє зв'язати все воедино і організувати управління з єдиної консолі. Система дає змогу скоротити час на виявлення можливих проблем, що можуть привести до збоїв у роботі обладнання та мережі в цілому.

Персоналу не потрібно переміщатися між кількома відкритими вікнами різних систем моніторингу, намагаючись звести кілька графіків і візуально оцінити ті чи інші закономірності і взаємозв'язок.

Рішення для централізованої системи моніторингу надає саме таку аналітичну інформацію, а також сигналізує про першопричини інцидентів у роботі обладнання і програмного забезпечення.

Одним з прикладів централізованої системи моніторингу є — IBM Netcool Network Management, що допомагає персоналу обслуговувати центри

обробки даних і мереж виявляти, візуалізувати, визначати, налаштовувати, активувати, виправляти і інтегрувати мережу.

Це єдине рішення комбінує IBM TivoliNetcool / OMNibus, IBM Tivoli Network Manager і IBM Tivoli Netcool Configuration Manager. [4]

Функції Netcool Network Management:

- один інтегрований набір інструментів управління мережею, який надає можливість сканування мережі, моніторингу, управління подіями і налаштування;
- централізоване подання інформації та створення звітів з охопленням складних, розподілених мережевих середовищ;
- сканування мережі і моніторинг, що дозволяють підвищити готовність і ефективність мережі;
- управління подіями і несправностями, які дозволяють швидко усунути мережеві несправності;
- можливості налаштування мереж, які підтримують ефективне розгортання та управління змінами.

Інтерфейс користувача

Кожна подія являє собою запис у таблиці попереджень.

Вид відображення налаштовується за допомогою фільтрів, що вказують які події будуть відображені і представлені, та відповідають за виведення на дисплей обраних стовпців з Object Server.

Є можливість встановити кілька сторінок зі списком подій, кожна з яких має різні пріоритети та фільтри. Фільтри дозволяють керувати процесом захоплення даних, і, так само, дозволяють економити простір буфера.

Залежно від значення певних полів пакета, заданих у вигляді умови фільтрації, пакет або ігнорується, або записується у таблицю. Використання фільтрів значно прискорює і спрощує аналіз, оскільки виключає перегляд непотрібних в даний момент повідомлень. Також можливо використовувати список подій для зміни пріоритету сповіщень, а також призначати або переназначати проблеми іншим користувачам. У смужці заголовка списку подій відображаються ім'я фільтра, який в даний час використовується для цього списку подій. Список подій відображає попередження в прокручуваному списку. Список подій наведено на рис. 3.

Node	Alert Group	Alert Description
link3	Link	Link Down on port
Sydney	Systems	Machine has gone offline
Moscow	Systems	Machine has gone offline
link2	Link	Link Down on port
London	Systems	Machine has gone offline
Washington	Systems	Machine has gone offline
Tokyo	Stats	Diskspace alert
Beijing	Stats	Diskspace alert
Tokyo	Stats	Diskspace alert
Beijing	Stats	Diskspace alert
Rome	Link	Port failure : port reset
London	Systems	Machine has gone online

Summary: 5 (green), 2 (purple), 6 (blue), 2 (yellow), 11 (orange), 0 (red), All Events

Status: 0 row(s) inserted, 22 row(s) updated | 03/15/08 12:24:16 | root PRESLEY[PR]

Рис. 3. Список подій

Список подій містить такі області:

1 — область попереджень, яка складається з рядків і стовпців у таблиці. Кожен рядок відповідає сповіщенню, який відповідає обраному зараз фільтру. Стовпці — поля попередження. Вибір стовпців регулюється поточним виглядом;

2 — стрічка підсумків розповсюдження відображає кількість сповіщень, які відповідають кожному кольору критичності.

Можна натиснути один з кольорів рівня критичності, щоб відображати лише ті сповіщення, які відповідають обраному рівню;

3 — рядок стану, де відображається: повідомлення про список подій, наприклад, кількість елементів, що відповідають поточному стану фільтра; поточна дата та час; поточне ім'я користувача для входу в сеанс.

В Netcool/Omnibus поняття «рівень критичності» (Severitylevel). Рівень критичності пов'язаний з кожним згенерованим повідомленням, щоб допомогти визначити пріоритети та керувати повідомленнями в списку подій. Рівні критичності —

кодування кольорів для легкої ідентифікації. Існує шість рівнів критичності за умовчанням, як показано в табл. 2 з можливими значеннями Clear, Indeterminate, Warning, Minor, Major та Critical.

Таблиця 2

Рівні критичності

Рівень	Значення	Колір
0	Clear	Зелений
1	Indeterminate	Фіолетовий
2	Warning	Блакитний
3	Minor	Жовтий
4	Major	Оранжевий

- Clear — рівень критичності, який використовують, коли стан помилки очищено.
- Indeterminate — рівень критичності, коли ступінь тяжкості стану помилки невідомий.
- Warning — рівень критичності, який використовується для позначення попередження тривоги.
- Minor — рівень критичності, що використовується для аварії незначної важкості.
- Major — рівень критичності, означає, що обладнання працює, але з сильно зниженою продуктивністю до точки, яка суттєво впливає на використання.
- Critical — рівень критичності, використовується для критичних аварій, означає, що обладнання не працює і потребує негайного втручання.

Оператори зв'язку зазвичай суміщають централізовану систему моніторингу з системою Trouble Ticketing — це система управління інцидентами та проблемами, що дозволяє здійснювати повну підтримку життєвого циклу усунення несправностей, простежити весь шлях події від її появи до завершення. Trouble Ticketing систематизує інформацію про кожну проблему, про способи та етапи її вирішення.

Функції:

- реєстрація дій персоналу щодо усунення несправностей;
- планування робіт з усунення несправностей;
- зв'язок інцидентів з аварійними повідомленнями, обладнання, на якому стався інцидент, постраждалими клієнтами і сервісами;
- оптимізація розподілу робіт по розв'язанню проблем між технічними фахівцями;
- контроль виконання завдань (пріоритет і статус проблеми, відповідальний, координатор, причина, вжиті заходи);
- облік часу щодо усунення несправностей;
- автоматична ескалація проблеми в разі перевищення заданих тимчасових інтервалів;

- уведення бази знань з проблем і методів їх рішень;
- моніторинг виконання робіт технічними фахівцями;
- гнучка система звітності для управлінських і технічних служб.

Такі системи зазвичай використовуються в мережевому операційному центрі (Network Operations Center — центр, що вирішує поточні завдання функціонування мережі, такі як моніторинг і управління, вирішення проблем, усунення аварійних ситуацій на мережі, підтримка користувачів і т. д.).

Висновки

Події і аварії є невід'ємним елементом експлуатації мережі. Оперативна діагностика і виявлення аварій є досить складним завданням, яке може бути вирішене тільки комплексом організаційно-технічних заходів. Розрізнені системи моніторингу, що використовують компанії, мають багато недоліків, які можуть бути вирішені впровадженням системи підтримки операційної діяльності. Такі системи, допомагають скоротити час на виявлення можливих проблем, які можуть привести до збоїв в роботі обладнання та інформаційних систем. Отримані події консолідується, доводяться до єдиного вигляду (нормалізуються), обробляються в реальному часі і зберігаються в окремій базі даних для звітів, з'ясування причин аварійних ситуацій, а також для детального аналізу параметрів якості мережі, які пов'язані з доступністю. Консолідація дозволяє бачити стан мережі через єдину консоль, а не розрізненими фрагментами в різних додатках і системах. У майбутньому планується детальний аналіз часу обробки інцидентів в мережі, шляхи автоматизації на обробку аварійних ситуацій, а також виділення основних критеріїв для успішної роботи системи підтримки операційної діяльності.

ЛІТЕРАТУРА

1. **Бреславський В. О.** Створення комплексної системи моніторингу з використанням аналізаторів сигналізацій телекомунікаційних систем // Наукові записки Українського науково-дослідного інституту зв'язку. — 2014. — №1(29). — С. 69–75.

2. **Одарченко Р. С.** Метод оцінки ключових показників захищеності в сучасних стільникових мережах / Р. С. Одарченко, В. О. Гнатюк, Д. Д. Вергелес, О. Ю. Скульська // Безпека інформації. — Вип. 1 (Т. 23), 2017. — С. 19–263.

3. Спайдер. Система распределенного мониторинга сетей связи. [Електронний ресурс] електронні текстові дані — режим доступу:

//<http://niits.ru/products/?spider>.

4. Netcool Network Management [Електронний ресурс] електронні текстові дані. — Режим доступу: // <https://www-03.ibm.com/software/products/ru/netcool-network-management>

5. Системы поддержки операционной деятельности — OSS [Електронний ресурс] електронні текстові дані — режим доступу: //<http://www.snt.ua/is/89988.ua.php> (18.02.2018).

6. What is OSS? In Chapter One of the Guide to Modern OSS we start at the very beginning: What is OSS and why is it needed? [Електронний ресурс] електронні текстові дані. — Режим доступу: //<http://www.ossline.com/what-is-oss> (18.02.2018).

Одарченко Р. С., Коберник А. Ю., Федюра Т. В.

ДОСЛІДЖЕННЯ АРХІТЕКТУРИ СУЧАСНИХ СИСТЕМ МОНІТОРИНГУ В МЕРЕЖАХ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

У статті досліджено OSS-рішення (Operations Support Systems), що дозволяють підвищити ефективність операційних процесів планування, будівництва і експлуатації мережі операторів зв'язку, а також дають змогу інженерам виконувати свою роботу швидше, ефективніше та якісніше. Забезпечення заданого рівня якості послуг і високої доступності обладнання мережі є одними з ключових завдань телекомунікаційного оператора. Проаналізовано, що швидке виявлення несправностей, ефективний пошук причин і визначення пріоритетів в їх усуненні є критичними для ефективного досягнення цієї мети. Виявлено, що у компаніях і організаціях, де використовуються розрізнені засоби моніторингу, відсутнє єдине уявлення про мережу, і як наслідок про вплив тієї чи іншої події на якість надання послуг. Оперативна діагностика і виявлення аварій є досить складним завданням, яке може бути вирішене тільки комплексом організаційно-технічних заходів. Впровадження системи підтримки операційної діяльності дозволяє, перш за все, скоротити час на виявлення можливих проблем, які можуть привести до збоїв в роботі обладнання та інформаційних систем. Централізована система моніторингу дозволяє зв'язати все воедино і організувати управління з єдиної консолі.

Ключові слова: OSS — Operations Support Systems; стільникова мережа; система моніторингу; QoS — quality of service.

Одарченко Р. С., Коберник А. Ю., Федюра Т. В.

ИССЛЕДОВАНИЕ АРХИТЕКТУРЫ СОВРЕМЕННЫХ СИСТЕМ МОНИТОРИНГА В СЕТЯХ СОТОВОЙ СВЯЗИ

В статье исследованы OSS-решения (Operations Support Systems), позволяющие повысить эффективность операционных процессов планирования, строительства и эксплуатации сети операторов связи, а также дают возможность инженерам выполнять свою работу быстрее, эффективнее и качественнее. Обеспечение заданного уровня качества услуг и высокой доступности оборудования сети являются одними из ключевых задач телекоммуникационного оператора. Проанализировано, что быстрое обнаружение неисправностей, эффективный поиск причин и определения приоритетов в их устранении являются критическими для эффективного достижения этой цели. Выведено, что в компаниях и организациях, где используются разрозненные средства мониторинга, отсутствует единое представление о сети, и как следствие влияния того или иного события на качество предоставления услуг. Оперативная диагностика и выявление аварий достаточно сложная задача, которая может быть решена только комплексом организационно-технических мероприятий. Внедрение системы поддержки операционной деятельности позволяет, прежде всего, сократить время на выявление возможных проблем, которые могут привести к сбоям в работе оборудования и информационных систем. Централизованная система мониторинга позволяет связать все воедино и организовать управление с единой консоли.

Ключевые слова: OSS — Operations Support Systems; сотовая сеть; система мониторинга; QoS — quality of service

Odarchenko Roman, Kobernik Anastasia, Fediura Tatyana

INVESTIGATION OF ARCHITECTURE OF CONTEMPORARY MONITORING SYSTEMS IN CELLULAR NETWORKS

In this paper, OSS solutions (Operations Support Systems) are investigated that allow to increase the efficiency of operational processes of planning, construction and operation of the network of telecom operators, and also enable engineers to perform their work faster, more efficiently and better. Providing a given level of service quality and high availability of network equipment is one of the key tasks of the telecommunications operator. It has been analyzed that the rapid detection of faults, the effective search for causes and the determination of priorities in their elimination are critical for the effective achievement of this goal. It has been revealed that in companies and organizations that use disparate monitoring tools, there is no unified view of the network, and as a consequence of the impact of an event on the quality of service provision. Operational diagnostics and the detection of emergencies are quite complex tasks that can be solved only by a set of organizational and technical activities. The introduction of the operational support system allows, first of all, to shorten the time to identify possible problems that can lead to malfunctions in the operation of equipment and information systems. Umbrella Fault Management allows you to tie everything together and organize management from a single console.

Keywords: OSS — Operations Support Systems; cellularnetwork; monitoringsystem; QoS — qualityofservice.

Стаття надійшла до редакції 14.05.2018 р.

Прийнято до друку 04.06.2018 р.

Рецензент — д-р техн. наук, проф. Коначович Г. Ф.