УДК 621.39:006.91 (02)

Бреславський В. О., асп., (Держ. універ.-т телекомунікацій. +380 (93) 322 96 73. slaava@i.ua)

СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ МОНІТОРИНГУ З ВИКОРИСТАННЯМ АНАЛІЗАТОРІВ СИГНАЛІЗАЦІЙ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Бреславський В. О. Створення комплексної системи моніторингу з використанням аналізаторів сигналізацій телекомунікаційних систем. Визначені основні задачі та підстави для розгляду питань створення комплексної системи моніторингу телекомунікаційних систем. Розглянута методологія проведення аналізу мережі, наведені приклади побудови систем аналізу і контролю вимірювань**.** Показано, що на сучасних телекомунікаційних мережах в даний час створено та експлуатуються одночасно декілька систем моніторингу. З метою здешевлення та спрощення існуючих систем моніторингу доцільно об'єднати їх в одну комплексну систему, використовуючи в якості базового елементу універсальний аналізатор сигналізацій телекомунікаційних систем (АСТС). Розглянуті особливості використання базового модуля збору інформації на базі АСТС з різним програмним забезпеченням і з єдиним центром обробки інформації про стан мережі. Описані функціональні характеристики систем контролю й вимірювань мережі сигналізацій «Сапсан» і «Спайдер»).

Ключові слова: телекомунікаційна мережа, моніторинг, аналізатор сигналізацій, вимірювання, якість обслуговування, аналіз мережі, Сапсан, Спайдер

Бреславский В. А. Создание комплексной системы мониторинга с использованием анализаторов сигнализаций телекоммуникационных систем. Определены основные задачи и основания для рассмотрения вопросов создания комплексной системы мониторинга телекоммуникационных систем. Рассмотрена методология проведения анализа сети, приведенные примеры построения систем анализа и контроля измерений**.** Показано, что на современных телекоммуникационных сетях в настоящее время создано и эксплуатируются одновременно несколько систем мониторинга. С целью удешевления и упрощения существующих систем мониторинга целесообразно объединить их в одну комплексную систему, используя в качестве базового элемента универсальный анализатор сигнализаций телекоммуникационных систем (АСТС). Рассмотрены особенности использования базового модуля сбора информации на базе АСТС с разным программным обеспечением и с единственным центром обработки информации о состоянии сети. Описаны функциональные характеристики систем контроля и измерений сети сигнализаций «Сапсан» и «Спайдер».

Ключевые слова: телекоммуникационная сеть, мониторинг, анализатор сигнализаций, измерения, качество обслуживания, анализ сети, Сапсан, Спайдер

Breslavskyy V. O. Creation of integrated monitoring system using the signalling analyzers of the telecommunication systems. The main tasks and reasons for consideration of items related to the creation of integrated monitoring system of the telecommunication systems are defined. It is considered the methodology of carrying out the network analysis and the examples of the analysis and measurements control systems engineering are given. It is shown that in the modern telecommunication networks are being created and operated simultaneously multiple monitoring systems. In order to reduce the cost and simplify the existing monitoring systems it is reasonable to combine them into one integrated system using the universal signalling analyzer of the telecommunication systems as a core element. The special aspects of application of a basic module collecting information on the basis of the telecommunication systems signalling analyzer with different software and with a single point of processing information related to network status are considered. The functional characteristics of the Sapsan and Spider signalling network control and measurement systems are described

Keywords: telecommunication network monitoring, signaling analyzer , measurement, quality of service, network analysis , Sapsan, Spader

Вступ. На теперішній час галузь телекомунікацій є напевно найбільш динамічно розвинутою. Безумовно, дане явище є позитивним з точки зору територіального поширення та доступності телекомунікаційних послуг та розширення їх спектру [1-3]. Кожен оператор, що працює на відкритому ринку, перебуває під тиском необхідності розширення спектру послуг, зростання трафіку і посилення конкуренції. Одним з недоліків цього процесу є те, що мережі стають все більш і більш складними, і при цьому, найчастіше, вони не мають адекватних засобів експлуатаційного управління. У таких мережах крім проблем керованості комутаційних пристроїв виникає необхідність гарантувати гарну якість мовлення, надійність встановлення з'єднання, виняток обривів розмови, високу швидкість передачі даних і т. п.

Однак, 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 доставці 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. Відомо, що створення і функціонування даної системи не є абстракцією або самоціллю, й повинно опиратися на техніко-економічні переваги і додаткові можливості, які повинні бути отримані при впровадженні 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 в будь-якому оточенні, зокрема, на різних апаратних платформах технічних засобів. ***Модульність*** забезпечує широкий спектр застосувань в залежності від потреб кінцевого споживача, не рахуючись з базовою версією платформи. Стабільні інтерфейси забезпечують взаємодію декількох прикладних систем (модулів) на єдиній платформі. ***Доступність*** забезпечує кінцевому споживачеві можливість у відповідності з потребами розвитку мережі (тобто, збільшення кількості елементів мережі) доповнювати систему комплексного моніторингу, витрачаючи на це мінімальні кошти.

Накопичуючи статистичні дані про параметри трафіку в окремих елементах мережі, система моніторингу дає можливість *контролювати* якісні показники мережі телекомунікацій, *планувати* її обслуговування і розширення, *управляти* мережею, *оперативно змінювати* конфігурацію мережі і т.п.

Крім того, система комплексного моніторингу дозволяє оптимізувати використання ресурсів мереж, а також планувати і реконфігурувати мережі з метою оптимізації маршрутизації трафіку та мінімізації можливих перевантажень;

Високі вимоги до якості послуг, оперативне підключення нових абонентів та розширення мережі ставлять перед операторами телекомунікацій принципово нові завдання безперервної оцінки показників використання мережі для її оптимізації, реконфігурації, розширення, визначення тарифної політики. Для ефективного управління мережами необхідно мати дані по будь-якому фрагменту мережі і, бажано в режимі реального часу. Система комплексного моніторингу на мережі дозволяє підвищити якість послуг, централізувати технічне обслуговування, оперативно планувати і впроваджувати розширення мережі, ефективно використовувати наявні ресурси.

Аналізатори протоколів та процес вимірювань. Простим способом неможливо звести в єдиний центр засоби управління і спостереження за пунктами сигналізації. Крім того, перебуваючи в режимі перевантаження, комутаційне обладнання може неадекватно відображувати стан елементів мережі ОКС-7 і IP-телефонії, а адже саме такі моменти представляють найбільший практичний інтерес при експлуатації мережі.

У зв'язку з цим, представляється доцільної побудова системи комплексного моніторингу, заснованої на пасивному підключенні до ланок ОКС-7, передачі даних. Принцип роботи такої системи використовує те, що інформацію про стан мережевих елементів, коливаннях сигнального навантаження і більшості інших параметрів, які повинні бути передані від мережевих елементів в центр спостереження для подальшого аналізу, можна отримати декодуючи повідомлення, які "знімаються" системою з ланки сигналізації. Розподілена система моніторингу здатна забезпечувати ряд додаткових функцій, наприклад таких, як виявлення фактів відведення та крадіжок трафіку і формування записів про виклик (Call Detail Record – далі CDR) для звірення рахунків при взаєморозрахунках між операторами.

Досвід проведення вимірювань на телекомунікаційних мережах показує, що для вимірювань доцільно використовувати універсальні і модульні аналізатори. Універсальність забезпечується максимально широким охопленням можливих вимірів, а наявність модульності програмного і апаратного забезпечень знижує вартість приладу. Враховуючи складність конфігурації приладів

цього класу, для реалізації необхідної методології їх необхідно вибирати з особливою ретельністю, залучаючи для цього кваліфікованих фахівців.

Сам процес аналізу протоколів включає захоплення циркулюючих в мережі пакетів, що реалізують той чи інший мережевий протокол, і вивчення вмісту цих пакетів. Ґрунтуючись на результатах аналізу, можна здійснювати обґрунтовану і зважену зміну будь-якого компонента мережі, оптимізацію її продуктивності, пошук і усунення неполадок. Відомо, що для того, щоб можна було зробити якісь висновки про вплив деякої зміни на мережу, необхідно виконати аналіз протоколів і до, і після внесення змін.

Аналізатор протоколів є самостійним спеціалізованим пристроєм, або персональним комп'ютером, зазвичай переносним, класу Notebook, оснащений спеціальною мережевою картою і відповідним програмним забезпеченням. Мережева карта і використовуване програмне забезпечення повинні відповідати топології мережі (кільце, шина, зірка). Аналізатор підключається до мережі точно так же, як і звичайний вузол. Відмінність полягає в тому, що аналізатор може приймати всі пакети даних, що передаються по мережі, в той час як звичайна станція – лише адресовані їй. Програмне забезпечення аналізатора складається з ядра, що підтримує роботу мережевого адаптера і декодує одержувані дані, та додаткового програмного коду, що залежить від типу топології досліджуваної мережі. Крім того, поставляється ряд процедур декодування, орієнтованих на певний протокол, наприклад, IPX. До складу деяких аналізаторів може входити також експертна система, яка може видавати користувачеві рекомендації про те, які експерименти слід проводити в даній ситуації, що можуть означати ті чи інші результати вимірювань, як усунути деякі види несправності мережі[1, 4-7].

Незважаючи на відносне різноманіття аналізаторів протоколів, представлених на ринку, можна назвати деякі риси, в тій чи іншій мірі притаманні всім їм:

- ***Інтерфейс користувача.*** Більшість аналізаторів мають розвинений дружній інтерфейс, який базується, як правило, на Windows. Цей інтерфейс дозволяє користувачеві: *виводити* результати аналізу інтенсивності трафіку; *отримувати* миттєву і середню статистичну оцінку продуктивності мережі; *задавати* певні події і критичні ситуації для відстежування їх виникнення; *робити* декодування протоколів різного рівня і представляти в зрозумілій формі вміст пакетів.
- ***Буфер захоплення.*** Буфери різних аналізаторів відрізняються за обсягом. Буфер може розташовуватися на мережевій карті, або для нього може бути відведено місце в оперативній пам'яті одного з комп'ютерів мережі. Якщо буфер розташований на мережевій карті, то управління ним здійснюється апаратно, і за рахунок цього швидкість введення підвищується. Однак це призводить до подорожчання аналізатора. У разі недостатньої продуктивності процедури захвату, частина інформації буде губитися, і аналіз буде неможливий. Розмір буфера визначає можливості аналізу по більш або менш представницьким вибіркам даних, що захоплюються. Але яким би великим не був буфер захоплення, рано чи пізно він заповниться. У цьому випадку або припиняється захоплення, або заповнення починається з початку буфера [1, 4, 5].
- ***Можливість вимірювання середньостатистичних показників*** трафіку в сегменті локальної мережі, в якому встановлений мережевий адаптер аналізатора.
- ***Вимірюється коефіцієнт використання*** сегменту, матриці перехресного трафіку вузлів, кількість нормальних і пошкоджених кадрів, що пройшли через сегмент.
- ***Можливість роботи з декількома агентами***, котрі поставляють захоплені пакети з різних сегментів локальної мережі. Ці агенти найчастіше взаємодіють з аналізатором протоколів за власним протоколом прикладного рівня.
- ***Фільтри.*** Фільтри дозволяють керувати процесом захоплення даних, і, тим самим, дозволяють економити простір буфера. Залежно від значення певних полів пакета, заданих у вигляді умови фільтрації, пакет або ігнорується, або записується в буфер захоплення. Використання фільтрів значно прискорює і спрощує аналіз, оскільки виключає перегляд непотрібних в даний момент пакетів.
- ***Перемикачі*** – це деякі умови початку і припинення процесу захоплення даних з мережі, що задаються користувачем. Такими умовами можуть бути виконання ручних команд запуску і зупинки процесу захоплення, тривалість процесу захоплення, поява певних значень в кадрах

даних. Перемикачі можуть використовуватися спільно з фільтрами, дозволяючи більш детально й тонко проводити аналіз, а також продуктивніше використовувати обмежений обсяг буфера захоплення.

• ***Пошук.*** Деякі аналізатори протоколів дозволяють автоматизувати перегляд інформації, що знаходиться в буфері, і знаходити в ній дані по заданим критеріям. У той час, як фільтри перевіряють вхідний потік на предмет відповідності умовам фільтрації, функції пошуку застосовуються до вже накопичених в буфері даних.

• ***Багатоканальність.*** Деякі аналізатори протоколів дозволяють проводити одночасний запис пакетів від декількох мережевих адаптерів, що зручно для зіставлення процесів, що відбуваються в різних сегментах мережі. Можливості аналізу проблем мережі на фізичному рівні у аналізаторів протоколів мінімальні, оскільки всю інформацію вони отримують від стандартних мережевих адаптерів. Тому вони передають і узагальнюють інформацію фізичного рівня, яку повідомляє їм мережевий адаптер, а вона багато в чому залежить від типу мережного адаптера. Деякі мережні адаптери повідомляють більш детальні дані про помилки кадрів та інтенсивності колізій в сегменті, а деякі взагалі не передають таку інформацію верхнім рівням протоколів, на яких працює аналізатор протоколів [1, 4, 5, 8].

Методологія проведення аналізу. Методологія проведення аналізу може бути представлена у вигляді наступних шести етапів:

- Захоплення даних.
- Перегляд даних, що були захвачені.
- Аналіз даних.
- Пошук помилок (більшість аналізаторів полегшують цю роботу, визначаючи типи помилок і ідентифікуючи станцію, від якої прийшов пакет з помилкою).
- Дослідження продуктивності. Розраховується коефіцієнт використання пропускної здатності мережі або середній час реакції на запит.
- Докладне дослідження окремих ділянок мережі. Зміст цього етапу конкретизується в міру того, як проводиться аналіз.

Зазвичай процес аналізу протоколів займає відносно небагато часу – 1-2 робочих дні.

На сьогоднішній день оператори телекомунікацій використовують кілька систем контролю та моніторингу мережі. Розглянемо ті з них, які беруть участь безпосередньо із забезпеченням сервісів голосової телефонії:

1) Системи контролю й вимірювань мережі сигналізацій (н-д, «Сапсан», «Спайдер»);
2) Система моніторингу IP- ресурсів;
3) Система контролю якості сервісів, в т.ч. голосової телефонії.

Система контролю і вимірювань мережі сигналізацій може використовуватися для таких цілей: *забезпечення* безперервного контролю за станом мережі сигналізації; *постійного* спостереження в режимі реального часу за елементами мережі сигналізації; *виявлення* і локалізації несправностей мережі сигналізації; *централізованого* контролю трафіку; *виявлення* незареєстрованої навантаження на об'єктах мережі; *виявлення* випадків несанкціонованого використання мережі сигналізації.

Зазначена система володіє багатими можливостями вибірки і фільтрації даних, використовуючи які, можливо отримувати значну кількість інформації.

Прикладом такої системи є «Спайдер» і «Сапсан» [9, 10, 11].

Метод незалежного збору даних, що застосовується у системі «Спайдер», надає всю ключову інформацію для оптимізації цифрових мереж TDM, NGN/IMS, GSM / GPRS, CDMA. Зібрана системою сигнальна інформація далі обробляється за допомогою високоефективних додатків, таких як: *моніторинг* мереж зв'язку, планування та оптимізація мережі; *мультипротокольне* трасування викликів; *збір* докладних записів про телефонні виклики, (транзакції і виклики); *контроль* узгоджених згідно SLA рівнів якості послуг, що надаються (SLA – угода про рівень якості надання послуг); *виявлення* несанкціонованого доступу до ресурсів мережі і зловмисних викликів; *моніторинг,* аналіз і комплексна експертна оцінка

роботи мереж VoIP; *кореляція* по протоколу MAP с CDR по протоколу ISUP (MAP – протокол сигналізації СКС-7; ISUP – підсистема сигналізації СКС-7) ; *моніторинг* загроз інформаційної безпеки мереж зв'язку з урахуванням специфіки застосовуваної на мережі технології.

Система «Спайдер» [11] використовує архітектуру клієнт/сервер, яка добре підходить для реалізації прийнятих логічних концепцій "агентів" і "менеджерів". Для обміну в реальному часі інформацією про стани об'єктів спостереження застосований протокол SMNP, а для обміну файлами даних – протокол HTTP.

Система «Сапсан» [9] також характеризується наявністю характеристик: великий перелік підтримуваних протоколів; *відстеження* викликів в масштабі реального часу; *централізований* контроль трафіку; *виявлення* незареєстрованого завантаження; *оновлення* конфігурації мережі та управління конфігурацією Системи з єдиного центру; *централізоване* відображення стану всієї мережі на одному екрані; *повідомлення* про аварійні ситуації в масштабі реального часу; отримання різних звітів; самоконтроль обладнання та ПЗ Системи.

Крім того, необхідно, щоб в системі моніторингу була присутня функція трасування викликів разом з функцією формування CDR-записів, яка є однією з найважливіших в системі моніторингу. Користувач системи задає телефонний номер (або частину номера), а система знаходить, групує за часом і видає всі сигнальні повідомлення, пов'язані з викликами на цей номер або з нього в межах всієї мережі. Причому трасування виклику може бути проведено як в реальному часі, так і в режимі постпроцесингу. Останнє можливо завдяки тому, що система моніторингу збирає і декодує всі сигнальні повідомлення, архівуючи і зберігаючи їх протягом декількох днів. Функції тригерів дозволяють зберігати результати трасування не для всіх викликів, а тільки для тих з них, які задовольняють заданому користувачем системи критерієм (час дня, цифри номера, причина роз'єднання, тривалість з'єднання і пр.), і тим самим на порядок підвищують інтервал безперервного спостереження [1, 5, 8].

Система моніторингу IP-ресурсів також виконує функції моніторингу IP-мережі, як правило, дозволяє здійснювати: *виявлення* проблем з відгуком додатків для кінцевого користувача; *ізолювання* причин зниження продуктивності IT-інфраструктури до рівня: мережа, сервер, користувач, додаток; *визначення* користувачів і додатків, що завантажують мережеві інтерфейси; *відстеження* внутрішніх параметрів мережевих пристроїв (комутатори, маршрутизатори, сервери); *відстеження* внутрішніх і зовнішніх загроз; *контроль* дотримання внутрішніх або зовнішніх SLA (угода про рівень якості надання послуг); *ведення* багаторівневої звітності про функціонування IT-інфраструктури.

Система контролю якості сервісів, в т.ч. голосової телефонії, **я**к правило, базується на отриманні інформації про параметри якості послуг голосової телефонії, яка передається по каналах електрозв'язку і по IP-мереж.

Даний напрямок є новим для телекомунікаційного ринку України і ще не зовсім поширений на мережах операторів.

Однак існують технологічні рішення, що дозволяють вимірювати показники, що характеризують доступність послуг для голосової телефонії, такі як: *відсоток* неуспішних викликів; *рівень* якості обслуговування (QoS) в VoIP мережі; *коефіцієнт* втрат пакетів, затримок, спотворення звуку (jitter), часу проходження сигналу, а також обчислення усередненої оцінки якості (Mean Opinion Score); *встановлений* час завершення з'єднання; *відсоток* викликів, які відповідають встановленим нормам за часом завершення з'єднання.

Опис основного елементу системи. Розглянувши основні параметри, які можуть збирати та аналізувати вищенаведені системи, можливо прийти до висновку, що сам пристрій, що збирає первинну інформацію і перенаправляє її для подальшої обробки може мати однакову апаратну складову, що має незначні відмінності. Технічно можливо встановити один пристрій типу аналізатора сигналізацій телекомунікаційних систем (АСТС) [9, 10], який можна підключити різними типами інтерфейсів одночасно до фрагментів мереж з традиційною телефонією, а так само до мереж передачі даних. АСТС забезпечує можливості декодування сигнальної інформації

в мережах відповідно до національних і міжнародних рекомендацій ITU –T та ETSI [12-15]. АСТС підтримує різні фізичні інтерфейси - E1, Ethernet, SDH (STM-1/4).

Завдяки архітектурі і закладеним спочатку принципам, АСТС є не лише потужним засобом локального контролю мережі ОКС-7, але і володіє системними функціями.

В якості базового елементу для збору первинної інформації можна використовувати АСТС, який зображений на Рис. 1.

Рис. 1. Базовий елемент

Все це робить можливим використання АСТС в якості бази для створення системи контролю та вимірювань.

У такому випадку АСТС в промисловому виконанні встановлюється в 19" стійку з доукомплектуванням спеціальним обладнанням системи моніторингу [9, 10].

Такий підхід дозволяє узагальнювати інформацію з декількох АСТС для централізованого використання, передавати в центр в реальному режимі часу дані про стан контрольованих об'єктів мережі, підготовляти звіти, що характеризують цілі сегменти мережі. Таким чином, забезпечується плавний перехід від покриття мережі локальними засобами до нової якості контролю – системи моніторингу мережі. При цьому локальні пункти системи моніторингу розвиваються на базі існуючих АСТС, укомплектованих відповідним чином.

Система моніторингу здатна виявляти перевантаження і аналізувати причини їх виникнення в різних точках мережі, на різних рівнях стека протоколів, у різних підсистемах. Граничні умови видачі сповіщень про перевищення заданого порогу, що настроюються безпосередньо користувачем, дають можливість завчасно надати інформацію для своєчасного перерозподілу наявних ресурсів, запобігаючи тим самим виникнення критичних перевантажень.

Доцільно підключити декілька АСТС (залежно від розміру мережі) на різних фрагментах мережі і встановити на них програмне забезпечення, що дозволяє здійснювати захоплення і первинну обробку даних на телекомунікаційних мережах.

Такі підключення можна розглядати як ланку (ланки) *першого рівня* комплексної системи моніторингу.

До *другого рівня* архітектури зазначеної системи можна віднести сервери баз даних з встановленим спеціальним програмним забезпеченням, що дозволяє здійснювати обробку отриманих даних з розташованих в різних місцях АСТС за різними критеріями (маршрутизація, стан мережі, якість голосових сервісів).

Крім того, однією з переваг архітектури такої системи є те, що комплексна система моніторингу є пасивною системою, що не робить впливу на роботу комутаційних систем, її робота не залежить від типів комутаційного обладнання і може виступати джерелом первинних даних для інших додатків.

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 в центр по виділеній підмережі передачі даних;

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

Архітектура Системи комплексного моніторингу гнучка, дворівнева.

Розробка і впровадження комплексної системи моніторингу телекомунікаційних мереж вимагає значних витрат. Їх обґрунтування і розрахунки економічних показників системи управління можливі на етапі конкретного проектування. Однак загальну оцінку витрат можна представити, стежачи за шляхами створення і тенденціями розвитку систем моніторингу в інших країнах.

Висновок. З метою зменшення витрат на моніторинг телекомунікаційної мережі доцільно створити єдину мережу комплексного моніторингу телекомунікаційної мережі, яка дозволить об'єднати декілька (2-3 різних мережі) в одну, використавши при цьому єдиний базовий модуль збору інформації на базі АСТС з різним програмним забезпеченням і з єдиним центром обробки інформації про стан мережі. При цьому термінали обробки наявних даних можуть бути розміщені в різних службах оператора і використовуватися для вирішення різних завдань широкого спектра, як для протидії "фроду" (вид шахрайства в області інформаційних технологій) до фізичного стану елементів мережі на предмет їх цілісності та пропускної здатності.

Література

1. Величко В. В. Телекоммуникационные системы и сети: Учебное пособие в 3 томах. Том 3. Мультисервисные сети / В. В. Величко, Е. А. Субботин, В. П. Шувалов, А. Ф. Ярославцев; под ред. профессора В. П. Шувалова. – М. Горячая линия-Телеком, 2005 – 592 с.

2. Системи та мережі цифрового радіозв'язку: інженерно-технічний довідник / [В. Ф. Олійник, В. Г. Кривуца, В. Г. Сайко, С. В. Булгач]. – Ніжин: ТОВ "Видавництво "Аспект-Поліграф", 2011. – 612 с.

3. Сайко В. Г. Практичні аспекти впровадження сучасних радіотехнологій WiMAX та радіорелейних систем / В. Г. Сайко, Ю. М. Літвінов // II науково-практична конференція «Актуальні питання регулювання у сфері телекомунікацій та користування радіочастотним ресурсом України». Київ, «Укрчастотнагляд», 11-13 червня 2008 р.). – С. 86.

4. Гольдштейн Б. С. Обеспечение безопасности сетей ОКС-7 / Б. С. Гольдштейн, И. М. Ехриель, Р. Д. Рерле [Електроний ресурс]. – Режим доступу : http://www.ccc.ru/magazine/depot/03_02/read.html?0302.htm (10.02.2014).

5. Инструменты мониторинга и анализа сети [Електроний ресурс]. – Режим доступу : // http://citforum.ru/nets/optimize/locnop_07.shtml (10.02.2014).

6. Сайко В. Г. Методичні та технічні аспекти визначення впливу електромагнітного випромінювання сучасних мобільних та безпроводових засобів цифрового зв'язку на здоров'я людини / В. Г. Сайко, Д. О. Дьомін, Д. О. Лисенко // Зв'язок. – 2010. – №1. – С.12-15.

7. Сайко В. Г. Особенности современных методов измерения удельной мощности излучения SAR, поглощаемой человеческим телом / В. Г. Сайко, Д. О. Лисенко // VI наукова конференція «Сучасні тенденції розвитку технологій в інфокомунікаціях та освіті», Київ, 05-06 листопада 2009 р. – С. 264.

8. Битнер В. И. Принципи та стандарты межсетевого взаимодействия. Учебное пособие / В. И. Битнер. – Новосибирск, «ВЕДИ», 2006. – 239 с.

9. Сапсан система контроля и измерений сети ОКС [Електроний ресурс]. – Режим доступу : // http://innovinn.com/downloads/innovinn_ss7.pdf (10.02.2014).

10. Системы мониторинга телекоммуникационных сетей [Електроний ресурс]. – Режим доступу : // http://www.innovinn.com/SolutionsMonitoring.aspx (10.02.2014).

11. Спайдер. Система распределенного мониторинга сетей связи [Електроний ресурс]. – Режим доступу : // http://niits.ru/products/?spider (10.02.2014).

12. Voice packetization – Packetized voice protocols // Recomendation ITU-T G.764 (12/90).

13. Packet circuit multiplication equipment // Recomendation ITU-T G.765 (09/92).

14. Signalling between circuit multiplication equip-ment's (CME) and international switching centers (ISC) // Recomendation ITU-T Q.50 (07/01).

15. Signalling system No.7 – Application transport mechanism: Bearer Independent Call Control (BICC) // Recomendation ITU-T Q.765.5 (04/04).