DOI 10.31891/2307-5732-2019-271-2-192-198
УДК 519.816

В. А. ДРУЖИНІН, В. О. МІЩЕНКО
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Ю. М. БОЙКО, О. М. РУБАН
Хмельницький національний університет

РОЛЬ ТА ЗАДАЧІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ МЕРЕЖЕЮ, ПОБУДОВАНОЮ ЗА ДОПОМОГОЮ БЕЗПРОВОДОВИХ РАДІОТЕХНОЛОГІЙ

Проаналізовано задачі, які виконують системи управління інформаційною мережею, визначена роль системи управління в інформаційній мережі, побудованій за допомогою безпроводових технологій. Проаналізовані алгоритми управління інформаційною безпекою та управління продуктивністю мережі. Поставлена задача дослідження. Описано фактори управління інформаційною мережею. Сформовано багаторівневе представлення завдань управління мережею.

Ключові слова: інформаційна мережа, управління інформаційною мережею, безпроводові радіотехнології, управління інформаційною безпекою, управління продуктивністю мережі.

V. A. DRUZHININ, V. O. MISCHENKO
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
J. M. BOIKO, O. M. RUBAN
Khmelnytskyi National University

DIRECTIONS AND TASKS OF INFORMATION MANAGEMENT BY NETWORK BASED ON RADIO TECHNOLOGIES

The tasks that are performed by the information network management systems were reviewed, the role of the management system in the information network that is built using wireless technologies was defined. The algorithms of information security management and network productivity management were analysed. The task of managing the information network should be divided at the level according to the hierarchical organization of the corporate network. The corporate network is constructed hierarchically, reflecting the hierarchy of the enterprise itself and its tasks. The lower level of the network consists of network elements - individual computers, communication devices, data channels. At the next level of the hierarchy, these elements form networks of different scales - the network of the working group, the network of the department, the network of the branch and, finally, the network of the enterprise as a whole. When managing the productivity of external and trunk communication channels, the most preferred is the use of a statistical approach to analysing the loading of information channels. It is based on a much smaller amount of information than is required by mass service theory, since as a research object only the load of the channel itself is taken, which is fixed at certain levels of time intervals. One of the ways to solve this problem is to use intelligent technologies to build an information and analytical system for monitoring information security systems information. The use of intelligent technologies will enable IT security professionals to analyse the processes of functioning of computer systems, to detect hidden semantic dependencies in data, to obtain models that allow estimating and predicting attempts of possible attacks and unauthorized connection in order to prevent them and thus increase the level the security of the computer system as a whole.

Keywords: information network, information network management, wireless radio technologies, information security management, network productivity management.

Вступ. Постановка завдання. Новітні засоби інформаційних послуг, які обумовлені все більшою інтеграцією інформаційних служб, потребують відповідних заходів щодо вдосконалення системи управління інформаційною мережею, у тому числі, побудованою за допомогою безпроводових радіотехнологій.

Розробка сучасних систем управління інформаційними мережами, побудованих за допомогою безпроводових радіотехнологій, є актуальним питанням, але в цьому питанні зроблені лише перші кроки. В Україні помітне суттєве відставання як у теорії, так і у практиці щодо управління інформаційними мережами, побудованими за допомогою безпроводових радіотехнологій, де дуже важливо забезпечити стале управління усіма елементами мережі [1–8].

Аналіз останніх досліджень і публікацій. Сьогодні важко знайти якусь галузь в Україні, де була б відсутня комп'ютерна мережа, яка має внутрішні інформаційні й обчислювальні ресурси та вихід до глобальної мережі. Що стосується системного телекомунікаційного оператора України, то роботи зі створення й забезпечення функціонування там інформаційних мереж провадяться вже багато років. Оскільки у теперішній час інформаційні мережі (ІМ) вже побудовані і функціонують, то на перший план виходить розв'язання задач їх гармонійного розвитку й ефективного використання мережевих ресурсів.

Розв'язуються ці задачі за допомогою засобів мережевого управління на базі використання системного підходу, який передбачає побудову цілісної системи управління, що розв'язує усі значимі задачі управління інформаційною мережею і не має слабких місць на окремих ділянках її компонентів.

Розглянемо роль та основні особливості інформаційної мережі, що впливають на побудову комплексної системи мережевого управління – інформаційна мережа системного телекомунікаційного оператора (ІМСТО) України, яка має корпоративну мережу, що об'єднує тисячі робочих станцій користувачів, десятки серверів і розподілена як всередині міст, так і по всій Україні.

Як наслідок, ІМСТО України має складну топологію, де використовуються канали передачі даних різної ємності, вона має вихід до глобальної мережі з використанням багатьох швидкодіючих каналів.

Накопичено великий об'єм різнорідних інформаційних ресурсів, що призначений як для внутрішніх, так і для зовнішніх користувачів. ІМСТО України забезпечує розв'язання великого числа задач з використанням різних мережевих застосувань та сервісів. Гостро стоять питання адміністрування різних категорій користувачів, забезпечення механізмів розподілу доступу до ресурсів. Обмежені можливості контролю за діяльністю користувачів, а також використання повністю централізованого механізму мережевого управління. В зв'язку з цим необхідний зважений підхід до модернізації ІМ, що полягає на забезпеченні принципу економічної доцільності та більш ефективного використання наявних програмних та апаратних засобів моделювання та оптимізації.

Основними задачами управління інформаційною мережею є [9]:

- управління безпекою;
- управління продуктивністю;
- облік використання ресурсів;
- управління збоями;
- моніторинг поточного стану ІМ, підтримка прийняття рішень з модернізації та управління модернізацією;
- моделювання роботи наявних мереж, зокрема аналіз навантаження на окремі її ділянки;
- управління конфігурацією.

Ключовими та першочерговими є розв'язки перших трьох задач: управління безпекою, управління продуктивністю та облік використання ресурсів. Інші задачі можливо розглядати як складові частини попередніх. Наприклад, система управління збоями може бути розглянута як підсистема системи управління безпекою, моделювання – як підсистема управління продуктивністю, а моніторинг необхідний як для розв'язку задач забезпечення продуктивності, так і безпеки.

Визначення факторів управління інформаційною мережею. Управління безпекою. Перш за все, визначимо загрози, які мають місце під час функціонування ІМ. Будь-яке порушення конфіденційності, цілісності, доступності інформаційних ресурсів, що негативно впливає на процес управління ІМСТО, є інцидентом безпеки, який необхідно своєчасно і правильно ідентифікувати з наступною реалізацією заходів для його усунення або зменшення можливої шкоди. Поняття інциденту вводиться міжнародним стандартом ISO/IEC 27001:2005, який узагальнює існуючі рекомендації і положення щодо організаційного забезпечення управління захистом інформаційної системи.

Сформулюємо основні поняття стандарту відповідно до ІМСТО України. Під інцидентом безпеки розуміється одинична подія або низка небажаних, непередбачених подій інформаційної безпеки, внаслідок яких існує велика імовірність компрометації результатів управління ІМСТО. Подія інформаційної безпеки – ідентифікований стан інформаційної мережі, який вказує на порушення політики інформаційної безпеки, відмову засобів захисту або раніше невідому ситуацію, яка може впливати на стан безпеки інформаційних ресурсів структурного підрозділу.

У загальному випадку реалізації інциденту безпеки відповідає певний стан інформаційної мережі, опис якого реєструється технічними засобами захисту. На підставі аналізу досвіду щодо ідентифікації інцидентів накопичується множина описів відомих ситуацій, що можуть бути використані в подальшому.

Необхідність розв'язання практичних задач щодо ідентифікації інцидентів обумовлена вимогами Нормативного документу технічного захисту інформації (НДТЗІ) 1.4–001–2000, який визначає множину функцій осіб зі складу служби захисту інформації [5–7]. Згідно з НДТЗІ можна визначити декілька функцій адміністратора безпеки:

- розслідування випадків порушення політики безпеки, подій безпеки та аналіз причин;
- реєстрація і моніторинг подій безпеки;
- проведення аналітичної оцінки поточного стану безпеки;
- негайне втручання в роботу інформаційної системи у випадку виявлення спроби реалізації загрози.

Для ефективної діяльності систем безпеки інформації потрібна її безперервна робота, а також всебічний контроль системи, яку потрібно захистити з боку адміністратора. У зв'язку з цим накопичується дуже великий файл з інформацією про діяльність самої системи та її користувачів, який в майбутньому і в найкоротший термін потрібно обробити. З досвіду можна сказати, що об'єм інформації, який потрібно обробити адміністратору безпеки, значно перевищує оптимальний об'єм, який адміністратор в змозі обробити. З цього випливає, що час реакції адміністратора системи безпеки на певну загрозу безпеці системи не дає змоги ефективно реагувати на події, що загрожують безпеці системі. Тобто потрібно автоматизувати рутинні операції обробки великої кількості подій щодо реагування на інциденти.

Методи аналізу інформації, що використовуються в сучасних системах моніторингу даних системи безпеки інформації є достатньо ефективними, якщо відомі точні характеристики подій. У ході дослідження було виявлено, що системи моніторингу даних системи безпеки інформації, наприклад, *IDES*, *IDIOT*, *STAT*, не можуть виявляти невідомі види атак. Всі вони передбачають застосування методів, що пов'язані з використанням статичних шаблонів відомих вторгнень: для виявлення нового виду вторгнення потрібно проінформувати систему про невідомий вид атаки – занести новий шаблон до її внутрішньої бази даних. Це є основним недоліком цих систем тому, що постійне втручання людини в процес виявлення вторгнень не дає бажаної ефективності роботи системи.

Системи моніторингу даних системи безпеки інформації зустрічаються з однаковою проблемою – характеристики атак, що постійно змінюються, потребують гнучкої захисної системи, яка була б спроможна залишатись ефективною, навіть якщо не відомі точні характеристики атаки. Більшість систем моніторингу даних системи безпеки інформації використовують один з підходів до виявлення вторгнень – виявлення аномалій або виявлення зловмисної діяльності користувачів. Оскільки методи, що реалізуються в рамках даних підходів, розраховані на виявлення чітко сформульованих типів атак, такі системи моніторингу даних системи безпеки інформації неодмінно зіштовхнуться з проблемою пропуску атак.

Отже, для ефективної роботи системи безпеки інформації потрібно автоматизувати роботу адміністратора системи безпеки інформації, а також використовувати методи, що давали б змогу реагувати на нові види атак.

Одним із способів розв'язання даної задачі є використання інтелектуальних технологій для побудови інформаційно-аналітичної системи моніторингу даних систем безпеки інформації. Використання інтелектуальних технологій дасть змогу фахівцям з безпеки інформаційних технологій аналізувати процеси функціонування комп'ютерних систем, виявляти приховані семантичні залежності у даних, отримувати моделі, що дозволяють оцінювати та прогнозувати спроби можливих атак та несанкціонованого підключення з метою їх запобігання і, таким чином, підвищити рівень захищеності комп'ютерної системи в цілому.

Інформаційно-аналітичні системи – це системи, що будуються на основі оперативних даних, що були отримані в режимі реального часу з оперативних систем, що автоматизують основні види діяльності організації, а також інших доступних джерел даних, які можуть знадобитися в ході прийняття стратегічних рішень. Базовий комплекс інформаційно-аналітичних систем торкається всієї управлінської вертикалі: звітності відділів та служб, аналізу їх діяльності, фінансово-економічного й стратегічного планування.

Інформаційно-аналітичні системи є надбудовою над уже функціонуючими інформаційними додатками, не роблячи особливого впливу на їхнє функціонування й не вимагаючи їхньої заміни. Ключовою функцією цих систем є акумулювання даних за всіма видами діяльності відділів та служб – від стану складів до фінансової й бухгалтерської звітності.

Побудову системи захисту ІМ необхідно створювати ешелоновано, розподіляючи наступні компоненти:

- Захист периметру мережі. Розв'язок цієї задачі забезпечується використанням міжмережевих екранів, які включають такі механізми: трансляція адрес для приховування структури та адресації внутрішньої мережі, фільтрація трафіку, управління списками доступу на маршрутизаторах, протидія атакам на внутрішні ресурси і т. ін.
- Захист серверів (внутрішніх та зовнішніх). Під час захисту поштових серверів обов'язковою вимогою є використання спеціальних антиспамових фільтрів, а також лексичних, репутаційних та сигнатурних аналізаторів. Одним з найпоширеніших у світі серверних спам-фільтрів є Symantec Brightmail Anti-Spam. Існують й інші комерційні фільтри – SpySweeper Enerprise, Cloudmark Immunity, NetIQ MailMarshal, MessageLabs Anti-Spam, Yandex «Спамооборона», Kaspersky Anti-Spam та інші. Рівень фільтрації спаму для цих продуктів коливається від 90% до 98%.
- Захист робочих станцій кінцевих користувачів. Зазвичай, при достатньому приділенні уваги до задач захисту периметру мережі та захисту серверів, забезпеченню захисту кінцевих робочих станцій приділяється мало уваги. Як наслідок, більша частина атак здійснюється як раз з робочих станцій кінцевих користувачів. Цю проблему допомагає вирішити використання персональних брандмаузерів та антивірусного програмного забезпечення. Лідируючи позиції у цьому секторі займають Symantec Norton Internet Security, продукти «Лаборатории Касперского» и Dr. Web.

Управління продуктивністю. Задачі управління продуктивністю можна розподілити на три класи: управління продуктивністю зовнішніх каналів, внутрішніх або локальних каналів, а також мережевих сервісів. При цьому особливу увагу треба приділити механізмам, направленим на удосконалення методів управління трафіком. Трафік (об'єм завантаження) кожного каналу зв'язку інформаційної мережі є важливим фактичним показником її роботи. Аналіз трафіку дозволяє оцінювати фактичне завантаження мережі і необхідну ємність її каналів, з'ясовувати стійкість роботи мережі і оперативність реакції на різні нештатні ситуації, судити про динаміку розвитку мережі і планувати терміни її модернізації.

До базових параметрів функціонування каналів передачі даних відносяться наступні показники, що розглядаються як в цілому, так і в розрізі щодо основних інформаційних сервісів: загальна кількість з'єднань протягом заданого невеликого інтервалу часу, загальний об'єм переданої інформації, загальна кількість переданих пакетів, а також загальний час з'єднань в цьому тимчасовому інтервалі. З тих, що є базовими показниками, легко будуються похідні показники, такі як швидкість передачі даних, обсяг завантаження каналу та ін. Одним з найважливіших показників функціонування інформаційних мереж є швидкість передачі даних кінцевим користувачам. Під цією величиною розуміється відношення кількості переданої інформації (у байтах) до сумарного часу передачі інформації за всіма з'єднаннями за фіксований проміжок часу. Таким чином, йдеться про усереднену швидкість передачі даних кінцевим користувачам за вибраний проміжок часу. Причому усереднювання ведеться не лише за проміжок часу, але і по всіх користувачах, які користувалися мережею в цей проміжок часу. Облік характеристик даної кривої дає мережевому адміністраторові і кінцевим користувачам можливість корегувати мережеву активність з

врахуванням поточного стану. Визначення усередненої швидкості передачі даних набуває особливої значимості, коли необхідно оцінити ефективність вживаних до мережі методів оптимізації трафіку.

Під час управління продуктивністю зовнішніх і магістральних каналів зв'язку найбільш переважним є використання статистичного підходу до аналізу завантаження інформаційних каналів. Він заснований на значно меншій кількості інформації, ніж вимагає теорія масового обслуговування, оскільки в якості об'єкту дослідження береться лише величина завантаження самого каналу, яка фіксується через певні рівні інтервали часу.

Для розв'язання цих завдань розроблена статистична модель внутрішньодобових коливань швидкості передачі даних [10]. Суть моделі полягає в тому, що дані про швидкість передачі, для якої спостерігаються значні коливання в сусідні проміжки часу, усереднюється за визначеним алгоритмом. Отримана в результаті усереднювання функція більш інформативна під час дослідження результатів дії на мережу. Враховуючи, що швидкість передачі даних залежить від активності користувачів, вона є нестаціонарним тимчасовим рядом, що має різні характеристики залежно від часу доби, дня тижня, місяця. У нашому випадку не має значення динаміка ряду, істотними є такі характеристики, як поведінка процесу протягом доби і часовий тренд.

Як показує аналіз тимчасового ряду швидкості передачі даних, даний ряд має періодичність, і схожі особливості ряду, які повторюються кожні 24 години. Прорахунок сезонної компоненти можна виробляти за однофакторною статистичною моделлю процесу, що описує почасове змінення швидкості передачі даних протягом доби. В якості 24 рівнів чинника в цій моделі необхідно розглядати різні часи доби. В якості оцінки сезонної компоненти в кожен момент часу в адитивній моделі тимчасового ряду можна розглядати середнє арифметичне різниці між середньогодинним значенням швидкості передачі даних і відповідним значенням ряду ковзаючих середніх.

Оскільки при управлінні потужністю зовнішніх каналів адміністратор мережі, як правило, має доступ до каналоутворюючого устаткування лише на одній стороні каналу, то управління може здійснюватись лише шляхом регулювання потоку інформаційних запитів від користувачів до зовнішніх мережевих сервісів. В ході управління продуктивністю локальних каналів можливе також використання статистичного підходу до аналізу, який, з одного боку, може бути джерелом здобуття вихідних даних для імітаційного моделювання, з іншого – для оптимізації управління.

Особливо слід зазначити можливість використання імітаційного моделювання з метою визначення найбільш ефективних дій, що управляють [11].

Облік використання ресурсів. Проблема обліку використання ресурсів Інтернет і контроль за роботою користувачів в мережі стоїть перед кожною організацією. Її вирішення залежить від типу організації, масштабу локальної мережі і кількості користувачів мережі Інтернет. Невеликі організації з декількома десятками користувачів використовують для обліку, в більшості випадків, програмне забезпечення, що вільно розповсюджується, рідше – власні розробки. Завдання системи побудови обліку використання ресурсів зводиться в основному до забезпечення взаєморозрахунків із зовнішніми Інтернет-провайдерами і до забезпечення контролю за роботою співробітників організації в мережі.

Найчастіше вживаним рішенням для крупних організацій і Інтернет-провайдерів є використання комерційних програмних продуктів, що мають відповідні сертифікати. Ці системи володіють хорошою масштабованістю і гнучкістю, що дозволяє побудувати їх під потреби організації. Функціональність подібних систем розширена за рахунок розвинених підсистем адміністрування користувачів, підсистем фінансового обліку і т. ін.

Проте використання подібних систем у деяких організаціях ускладнене з-за їх високої вартості, а також деяких обмежень, обумовлених строго визначеною моделлю обліку (наприклад, відсутність ієрархії груп користувачів). У цьому випадку доводиться або підлаштовуватись під відповідні обмеження, або займатися доопрацюванням подібних систем. Багато організацій вибирають шлях створення власних систем обліку, що повністю відповідають пред'явленим до них вимогам.

Взаємозв'язок компонентів системи мережевого управління. Зазначимо питання, що стосуються взаємодії компонентів системи мережевого управління, а також переваги, які дає системний і комплексний підхід до її реалізації:

- у всіх підсистемах необхідно використовувати єдину базу даних компонентів ІМ, інформаційних ресурсів і користувачів; це ключові компоненти, без створення яких неможливо вирішити питання створення системи управління ІМ;
- отримання статистичною інформації про поведінку трафіку в системі управління продуктивністю дозволяє виявити аномалії, що може з'явитися наслідком мережевих атак; отже, ефективність системи забезпечення безпеки може значно зрости під час використання подібної інформації;
- зниження продуктивності може бути наслідком надмірного завантаження каналів передачі даних за рахунок різкого збільшення об'єму використання ресурсів; тут очевидна взаємодія системи обліку використання ресурсів і системи управління продуктивністю;
- зниження продуктивності може бути наслідком мережевих атак. В даному випадку відзначимо взаємодію систем забезпечення безпеки і продуктивності;
- користувачі, в результаті аналізу статистики своєї роботи, можуть виявити факти несанкціонованого використання своїх облікових записів. Це зв'язок систем обліку використання ресурсів і

безпеки.

На закінчення необхідно відзначити, що комплексний системний підхід до даної проблеми все ж таки найбільш виправданий і це дозволяє побудувати основні компоненти системи мережевого управління в найкоротші терміни і з мінімальними витратами.

Багаторівневе представлення завдань управління. Завдання управління інформаційною мережею доцільно розділяти на рівні відповідно до ієрархічної організації корпоративної мережі. Корпоративна мережа будується ієрархічно, відображаючи ієрархію самого підприємства і його завдань. Нижній рівень мережі складають елементи мережі – окремі комп'ютери, комунікаційні пристрої, канали передачі даних. На наступному рівні ієрархії ці елементи утворюють мережі різного масштабу – мережа робочої групи, мережа відділу, мережа відділення і, нарешті, мережа підприємства в цілому.

Для побудови інтегрованої системи управління різнорідними елементами мережі природно застосувати багаторівневий ієрархічний підхід. Це, в принципі, стандартний підхід для побудови великої системи будь-якого типу і призначення – від держави до автомобільного заводу. Стосовно систем управління мережами, що найбільш пропрацював і ефективний для створення багаторівневої ієрархічної системи, є стандарт *Telecommunication Management Network* (*TMN*), розроблений спільними зусиллями *ITU-T*, *ISO*, *ANSI* і *ETSI*. Хоча цей стандарт і призначався спочатку для телекомунікаційних мереж, але орієнтація на використання загальних принципів робить його корисним для побудови будь-якої крупної інтегрованої системи управління мережами. Стандарти *TMN* складаються з великої кількості рекомендацій *ITU-T* (і стандартів інших організацій), але основні принципи моделі *TMN* описані в рекомендації *M*.3010.

Модель *TMN* спрощено можна уявляти у вигляді двомірної діаграми (рис. 1).

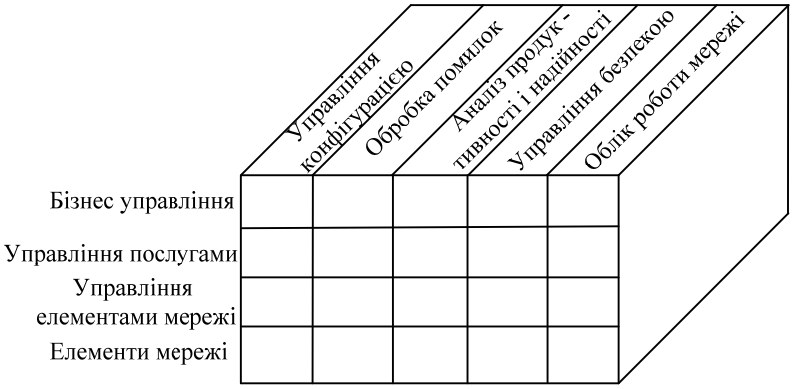

Рис. 1. Багаторівневе представлення завдань управління мережею

Нижній рівень – *рівень елементів мережі (Network Element layer, NE)* – складається з окремих пристроїв мережі: каналів, підсилювачів, кінцевої апаратури, мультиплексорів, комутаторів і тому подібного. Елементи можуть містити вбудовані засоби для підтримки управління – датчики, інтерфейси управління, а можуть і представляти собою засіб, що вимагає для зв'язку з системою управління розробки спеціального устаткування пристроїв зв'язку з об'єктом. Сучасні технології зазвичай мають вбудовані функції управління, які дозволяють виконувати хоч би мінімальні операції з контролю за станом пристрою і за переданим пристроєм трафіком. Подібні функції вбудовані в технології *FDDI*, *ISDN*, *frame relay*, *SDH*. В цьому випадку пристрій завжди можна охопити системою управління, навіть, якщо воно не має спеціального блоку управління, оскільки протокол технології зобов'язує пристрій підтримувати деякі функції управління. Пристрої, які працюють за протоколами, що не мають вбудованих функцій контролю і управління, забезпечуються окремим блоком управління, який підтримує один з двох найбільш поширених протоколів управління, – *SNMP* або *CMIP*. Ці протоколи відносяться до прикладного рівня моделі *OSI*.

Наступний рівень – рівень управління елементами мережі (*network element management layer*) – є елементарними системами управління. Елементарні системи управління автономно управляють окремими елементами мережі, контролюють канал зв'язку *SDH*, управляють комутатором або мультіплексором. Рівень управління елементами ізолює верхні шари системи управління від деталей і особливостей управління конкретним устаткуванням. Цей рівень відповідальний за моделювання поведінки устаткування і функціональних ресурсів мережі. Прикладами таких систем можуть служити системи управління *CiscoView* від *Cisco Systems*, *Optivity* від *Bay Networks, RADView* від *RAD Data Communications* і так далі.

Вище лежить рівень управління мережею (*Network management layer*). Цей рівень координує роботу елементарних систем управління, дозволяючи контролювати конфігурацію складених каналів, погоджувати роботу транспортних підмереж різних технологій і тому подібне. За допомогою цього рівня мережа починає працювати як єдине ціле, передаючи дані між своїми абонентами.

Наступний рівень – рівень управління послугами (*Service management layer*) – займається контролем і управлінням за транспортними і інформаційними послугами, які надаються кінцевим користувачам мережі. У завдання цього рівня входить підготовка мережі до надання певної послуги, її активізація, обробка викликів клієнтів. Формування послуги (*service provisioning*) полягає у фіксації в базі даних значень параметрів послуги, наприклад, необхідної середньої пропускної спроможності, максимальних величин

затримок пакетів, коефіцієнта готовності і тому подібного. У функції цього рівня входить також видача рівню управління мережею завдання на конфігурацію віртуального або фізичного каналу зв'язку для підтримки послуги.

Рівень бізнес-управління (*Business management layer*) займається питаннями довготривалого планування мережі з урахуванням фінансових аспектів діяльності організації, мережею, що володіє. На цьому рівні щомісячно і поквартально підраховуються доходи від експлуатації мережі і її окремих складових, враховуються витрати на експлуатацію і модернізацію мережі, приймаються вирішення про розвиток мережі з урахуванням фінансових можливостей. Рівень бізнес-управління забезпечує для користувачів і постачальників послуг можливість надання додаткових послуг. Цей рівень є окремим випадком рівня автоматизованої системи управління підприємством (АСУП), тоді як всі нижчі рівні відповідають рівням автоматизованої системи управління технологічними процесами (АСУТП), для такого специфічного типу підприємства, як телекомунікаційна [12, 13] або корпоративна мережа. Але, якщо телекомунікаційна мережа дійсно найчастіше є основою телекомунікаційної компанії, то корпоративну мережу і обслуговуючий її персонал зазвичай важко назвати підприємством.

Висновки

1. Для реалізації безпроводових радіотехнологій важливо забезпечити стале управління усіма елементами мережі.

2. На поточний момент реалізація безпровідних технологій пов’язана з розв’язанням задач їх гармонійного розвитку й ефективного використання мережевих ресурсів.

3. Для ефективної роботи системи безпеки інформації потрібно автоматизувати роботу адміністратора системи безпеки інформації, зокрема шляхом використання інтелектуальних технологій для побудови інформаційно-аналітичної системи моніторингу даних.

4. Найважливішим показником функціонування інформаційних мереж є швидкість передачі даних кінцевим користувачам. Під час управління продуктивністю зовнішніх і магістральних каналів зв'язку найбільш переважним є використання статистичного підходу до аналізу завантаження інформаційних каналів.

5. Багато організацій вибирають шлях створення власних систем обліку, що повністю відповідають пред'явленим до них вимогам.

6. Пристрої, які працюють по протоколах, що не мають вбудованих функцій контролю і управління, забезпечуються окремим блоком управління, який підтримує один з двох найбільш поширених протоколів управління, – *SNMP* або *CMIP*.

Література

1. Олифер Н. А. Средства анализа и оптимизации локальных сетей / Н. А. Олифер, В. Г. Олифер. – Центр Информационных Технологий, 1998. – 424 с.

2. Герасимов Б. М. Аналіз задач моніторингу інформаційних мереж та методів підвищення ефективності їх функціонування / Б. М. Герасимов, І. Ю. Субач, П. В. Хусаінов, В. О. Міщенко // Сучасні інформаційні технології у сфері безпеки та оборони . – 2008. – № 3 (3). – С. 24–27.

3. Кільчицький Є. В. Властивості та критерії оцінювання ефективності сучасної автоматизованої системи управління телекомунікаціями / Є. В. Кільчицький // Зв’язок. – 2003. – № 1. – С. 9–12.

4. Бойко Ю. М. Концептуальні особливості реалізації безпровідних сенсорних мереж / Ю. М. Бойко, В. М. Локазюк, В. В. Мішан // Вісник Хмельницького національного університету. Технічні науки. – 2010. – № 2. – С. 94–98.

5. Герасимов Б. М. Системы поддержки принятия решений: проектирование, применение, оценка эффективности / Б. М. Герасимов, М. М. Дивизинюк, И. Ю. Субач // НАН Украины НИЦ ВС Украины Государственный океанариум, 2004. – 318 с.

6. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – [Введ. 28.04.1999]. – К. : ДСТСЗИ СБ Украины, 1999.

7. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. – [Введ. 28.04.1999]. – К. : ДСТСЗИ СБ Украины, 1999.

8. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. – [Введ. 04.12.2000]. – К. : ДСТСЗИ СБ Украины, 2000.

9. Замятин В. С. Принципы построения комплексной системы управления информационно-вычислительной сетью ВУЗа / В. С. Замятин // Ползуновский вестник. – 2006. – № 2. – С. 60–67.

10. Замятин В. С. Использование статистического подхода при решении задач анализа и управления компьютерными сетями / В. С. Замятин // Известия АГУ. – 2003. – № 1. – С. 54–57.

11. Данилюк Ю. С. Система моделирования локальных вычислительных сетей / Ю. С. Данилюк, Ф. А. Попов // Изв. АГУ: Спецсборник. – 2002. – С. 63-64.

12. Boiko J. Signal Processing in Telecommunications with Forward Correction of Errors / J. Boiko, O. Eromenko // Indonesian Journal of Electrical Engineering and Computer Science. – 2018. – Vol. 11, nr. 3. – P. 868–877. – DOI: http://doi.org/10.11591/ijeecs.v11.i3.pp868-877.

13. Boiko J. Productivity of telecommunication systems with modified signal-code constructions / J. Boiko,

I. Kovtun, S. Petrashchuk // Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International. – IEEE, 2017. – С. 173–178. – DOI: 10.1109/INFOCOMMST.2017.8246374.

References

1. Olifer N. A. Sredstva analiza i optimizacii lokal'nyh setej / N. A. Olifer, V. G. Olifer. – Centr Informacionnyh Tehnologij, 1998. – 424 s.

2. Herasymov B. M. Analiz zadach monitorynhu informatsiinykh merezh ta metodiv pidvyshchennia efektyvnosti yikh funktsionuvannia / B. M. Herasymov, I. Yu. Subach, P. V. Khusainov, V. O. Mishchenko // Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony . – 2008. – № 3 (3). – С. 24–27.

3. Kilchytskyi Ye. V. Vlastyvosti ta kryterii otsiniuvannia efektyvnosti suchasnoi avtomatyzovanoi systemy upravlinnia telekomunikatsiiamy / Ye. V. Kilchytskyi // Zviazok. – 2003. – № 1. – S. 9–12.

4. Boiko Yu. M. Kontseptualni osoblyvosti realizatsii bezprovidnykh sensornykh merezh / Yu. M. Boiko, V. M. Lokaziuk, V. V. Mishan // Herald of Khmelnytskyi National University. – 2010. – № 2. – S. 94–98.

5. Gerasimov B. M. Sistemy podderzhki prinjatija reshenij: proektirovanie, primenenie, ocenka jeffektivnosti / B. M. Gerasimov, M. M. Divizinjuk, I. Ju. Subach // NAN Ukrainy NIC VS Ukrainy Gosudarstvennyj okeanarium, 2004. – 318 s.

6. ND TZI 1.1-002-99. Zahalni polozhennia shchodo zakhystu informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu. – [Vved. 28.04.1999]. – K. : DSTSZY SB Ukraыnы, 1999.

7. ND TZI 1.1-003-99. Terminolohiia v haluzi zakhystu informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu. – [Vved. 28.04.1999]. – K. : DSTSZY SB Ukraыnы, 1999.

8. ND TZI 1.4-001-2000. Typove polozhennia pro sluzhbu zakhystu informatsii v avtomatyzovanii systemi. – [Vved. 04.12.2000]. – K. : DSTSZY SB Ukraыnы, 2000.

9. Zamjatin V. S. Principy postroenija kompleksnoj sistemy upravlenija informacionno-vychislitel'noj set'ju VUZa / V. S. Zamjatin // Polzunovskij vestnik. – 2006. – № 2. – С. 60–67.

10. Zamjatin V. S. Ispol'zovanie statisticheskogo podhoda pri reshenii zadach analiza i upravlenija komp'juternymi setjami / V. S. Zamjatin // Izvestija AGU. – 2003. – № 1. – S. 54–57.

11. Daniljuk Ju. S. Sistema modelirovanija lokal'nyh vychislitel'nyh setej / Ju. S. Daniljuk, F. A. Popov // Izv. AGU: Specsbornik. – 2002. – S. 63-64.

12. Boiko J. Signal Processing in Telecommunications with Forward Correction of Errors / J. Boiko, O. Eromenko // Indonesian Journal of Electrical Engineering and Computer Science. – 2018. – Vol. 11, nr. 3. – P. 868–877. – DOI: http://doi.org/10.11591/ijeecs.v11.i3.pp868-877.

13. Boiko J. Productivity of telecommunication systems with modified signal-code constructions / J. Boiko, I. Kovtun, S. Petrashchuk // Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International. – IEEE, 2017. – S. 173–178. – DOI: 10.1109/INFOCOMMST.2017.8246374.

Рецензія/Peer review : 20.2.2019 р. Надрукована/Printed :10.4.2019 р.
Стаття прорецензована редакційною колегією