УДК 623.486

Ірина КОНОНОВА,
Військовий інститут телекомунікацій та інформатизації, м. Київ

АНАЛІЗ ВПЛИВУ ЗБОЇВ НА НАДІЙНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ МЕРЕЖ ЗВ'ЯЗКУ

Проведено аналіз впливу збоїв на надійність телекомунікаційного обладнання мереж зв'язку. Показано, що ігнорування збоїв програмного забезпечення телекомунікаційного обладнання може призвести до суттєвих втрат часових та людських ресурсів. Тому в оцінці показників надійності сучасних мереж зв'язку необхідно враховувати збої у роботі протоколів маршрутизації і у програмному забезпеченні телекомунікаційного обладнання.

Ключові слова: *мережа зв'язку, показники надійності, протоколи маршрутизації, відмова, збій.*

Аналіз останніх досліджень та публікацій, в яких започатковано вирішення даної проблеми та на які опирається автор. До теперішнього часу в більшості фахівців у галузі телекомунікаційних мереж сформувалася думка про недоцільність проведення наукових досліджень і застосування практичних заходів, пов'язаних з кількісною оцінкою та забезпеченням надійності цього класу технічно складних систем [1–5]. Зневага до питань надійності нерідко обґрунтовується тим, що сучасні засоби зв'язку є досить надійними, а мережі зв'язку – розгалуженими та такими, які допускають обходи. З цим можна част-

ково погодитись, однак кожен етап розвитку техніки ставить на порядок денний нові задачі, які вимагають свого розв'язку. Це повною мірою стосується і до забезпечення надійності мереж зв'язку.

Метою статті є аналіз впливу збоїв на надійність телекомунікаційного обладнання (ТЛКО) мереж зв'язку.

Виклад основного матеріалу дослідження. На даний час відбуваються істотні зміни в технологіях зв'язку. На зміну комутації каналів приходить комутація пакетів, активно впроваджуються нові технології транспорту та доступу, застосовуються нові протоколи. Важливою перевагою мереж, які використовують IP протокол, є можливість надавати безліч альтернативних шляхів передачі інформації. Саме тому у роботах [6-8] зроблено висновок щодо переваг рішень IP протоколу з точки зору надійності. Але у дійсності це не більш ніж міф [8].

Для реалізації вказаної переваги необхідно мати достатньо розгалужену фізичну інфраструктуру. Тільки у цьому випадку різні шляхи будуть розподілені не тільки логічно, але і фізично. Інакше вони можуть проходити, наприклад, у загальному кабелі, обрив якого призведе до непрацездатності усіх шляхів.

Крім цього, час переходу на нові шляхи передачі інформації у мережах IP занадто великий для трафіку реального часу, і якщо не приймати додаткових мір захисту, таке переключення призведе до розривів з'єднань. Тому механізми швидкого відновлення часто реалізуються на фізичному рівні. А саме тут спостерігається перехід від технології SDH, що має різні стандартизовані механізми резервування, які забезпечують високу відмовостійкість мережі, до більш дешевої, але такої, що не має доки подібних механізмів технології Ethernet.

Суттєвою особливістю мереж IP з точки зору надійності є те, що в них поряд з надійністю телекомунікаційного обладнання та надійністю інфраструктури мережі IP з'являється нове джерело відмов – збої у роботі протоколів маршрутизації і у програмному забезпеченні телекомунікаційного обладнання мереж зв'язку (маршрутизатори, комутатори, концентратори та інше).

Протоколи маршрутизації дуже чутливі до помилок конфігурування [7]. При цьому у звіті Проблемної групи з NGN Консультатив-

ного комітету зі зв'язку для національної безпеки при Президентові США звертається увага, що через особливості роботи протоколів маршрутизації такі порушення можуть розповсюджуватися у мережі зв'язку лавиноподібно [9]. Прикладом цього є вихід з ладу значної частини мережі IP японського оператора зв'язку NTT [10]. При цьому до 4 тис. маршрутизаторів виробництва Cisco перебували у непрацездатному стані близько 7 годин. Першопричиною випадку стало переключення на резервні маршрути, яке викликало некоректне оновлення таблиць маршрутизації, що і призвело до масової непрацездатності маршрутизаторів.

Помилки у програмному забезпеченні телекомунікаційного обладнання також суттєво впливають на надійність функціонування мережі загалом. Основними причинами, які викликають порушення нормального функціювання програми, є помилки, що скриті у самій програмі; спотворення вхідної інформації, яка підлягає обробці; невірні дії користувача [11].

Зазвичай у технічних умовах на телекомунікаційне обладнання відсутні дані щодо надійності програмного забезпечення. Це пов'язано з тим, що неможливо передбачити та заздалегідь перевірити всі поєднання вихідних даних, які виникають при експлуатації програм і даних, що передаються за допомогою мережних протоколів.

У загальному випадку критеріями відмови програмного забезпечення необхідно вважати припинення функціонування програми (спотворення нормального ходу її виконання, зациклення) на час, що перевищує допустиме значення $t_д$, або на час, що не перевищує допустиме значення $t_д$, але з втратою усіх або частини оброблювальних даних чи з необхідним перезавантаженням ЕОМ, на якій функціює програмне забезпечення [11]. Оскільки відновлення працездатності стану програмного забезпечення може виникнути без втручання оператора (перезавантаження ЕОМ, маршрутизатора, комутатора, концентратора і т. д. не вимагається) або ж за участю оператора чи експлуатуючого персоналу (перезавантаження ЕОМ, маршрутизатора, комутатора, концентратора і т. д. необхідне), тоді всі відмови у програмному забезпеченні можна трактувати як збої. У ДСТУ [12] під збоєм розуміється

самоусувна відмова або одноразова відмова, яку незначним втручанням усуває оператор, тобто короткочасне порушення працездатності програмно-керувальних розрахункових комплексів, за якого функціювання відновлюється без проведення ремонтних робіт.

Наведені вище критерії відмов призводять до необхідності аналізу часових характеристик функціювання програми і динамічних характеристик телекомунікаційного обладнання, отриманих у ході функціювання програмного забезпечення. Граничний час відновлення (допустимий час відновлення $t_{\text{д}}$) працездатного стану системи, у разі перевищення якого необхідно фіксувати відмову (зрив функціонування), близький до періоду вирішення задач для підготовки інформації (даних) відповідного телекомунікаційного обладнання. Отже, для будь-якого телекомунікаційного обладнання існує допустимий час відсутності даних від програми, за якого його характеристики знаходяться у допустимих межах. Виходячи з цього часу, можна встановити границі часової зони, яка розділяє працездатний та непрацездатний стан програмного забезпечення і дозволяє використовувати ці границі як критерій відмов (зривів функціонування).

При цьому слід ураховувати, що час відновлення функціонування програмного забезпечення складається не тільки з часу, необхідного для перезавантаження телекомунікаційного обладнання та завантаження самого програмного забезпечення, але і з часу, необхідного для відновлення даних (наприклад, оновлення таблиць маршрутизації), і цей час у ряді випадків може значно перевищувати час перезавантаження.

Ігнорування збоїв програмного забезпечення телекомунікаційного обладнання при аналізі надійності мережі зв'язку може призвести до суттєвих втрат часових та людських ресурсів. Наведемо приклади.

1. Під час першої війни в Перській затоці американській системі протиракетної оборони Patriot, встановленої в Саудівській Аравії, не вдалося перехопити атаку іракських ракет Скад (Scud). Ракетами були знищені армійські казарми і солдати, які в них перебували під час атаки.

Причина – помилка програмного забезпечення. Через некоректне округлення (при переводі десятих часток секунди в секунди) було неправильно розраховано час, у результаті чого система Patriot просто проіг-

норувала ракети Scud, що наближалися. Похибка склала всього близько 0,34 секунди, але за цей час ракета долає відстань у півкілометра.

2. Через незначні механічні пошкодження відмовив всього один телефонний комутатор в одному з 114 центрів зв'язку найбільшої телефонної компанії США – AT&T, а в результаті перестав функціонувати весь центр зв'язку. Коли через деякий час центр відновив роботу, він автоматично відправив повідомлення всім іншим комутаційним центрам, які, у свою чергу, також припинили роботу і зупинили всю мережу AT&T на 9 годин.

Причина – один помилковий рядок в програмному коді у комплекті оновлення програмного забезпечення, призначеного для прискорення виклику, породив незвичайний хвильовий ефект, який змусив замовчати цілу телефонну мережу.

3. Збій у системі глобального позиціонування GPS призвів до проблем у роботі навігаційного обладнання та системах зв'язку в усьому світі. Інцидент стався наприкінці січня 2016 року, відразу після того, як Військово-повітряні сили США вивели зі складу угруповання супутник SVN 23 для його подальшої заміни на GPS Block IIF. Збій, який призвів до проблем обладнання, пройшов глобально по всьому світу в різний час зі зміщенням, що відповідав тому, як супутники GPS рухалися вздовж своїх орбіт. Тривалість цього інциденту склала близько 12 годин. Обладнання операторів зв'язку стало видавати попередження обслузі персоналу, причому кількість цих попереджень збільшувалася за наростаючою. У ряді випадків уникнути серйозних наслідків допомогли резервні системи синхронізації часу.

Причина – у ході процедури в програмному забезпеченні, яке застосовується в наземній інфраструктурі GPS, виник збій, у результаті якого на 13 мікросекунд сталося відключення переданого GPS супутниками сигналу Всесвітнього координованого часу [13].

4. Наслідки збою в GPS можна порівняти з наслідками, що виникли внаслідок відмови російської навігаційної системи ГЛОНАСС, яка сталася в квітні 2014 року і тривала близько 10 годин.

Причина – помилкове завантаження коригувальних даних супутника ГЛОНАСС.

Ці та інші приклади показують, що навіть малі відхилення в складній системі, викликані збоями, здатні призвести до ненавмисних глобальних наслідків, а також обґрунтовують гостру необхідність враховувати збої програмного забезпечення в оцінці надійності телекомунікаційного обладнання мереж зв'язку.

Мережа зв'язку становить собою складну технічну систему, яка складається з великої кількості взаємопов'язаних елементів [14]. Елементом мережі зв'язку може вважатися апаратура каналоутворення (канали зв'язку), пристрої комутації та маршрутизації, сервери, робочі станції, апаратура IP шифрування, кінцеве обладнання (телефонні апарати, термінали зв'язку і т. д.). У той же час, розглядаючи функціювання маршрутизаторів різних рівнів, комутаторів, серверів, робочих станцій, можна виділити в цих пристроях процесори, оперативну пам'ять, пристрої введення-виведення, різні інтерфейси.

Проведене дослідження [16], яке розглядало різноманітні обчислювальні платформи від безлічі виробників, а також різні типи динамічної пам'яті, включаючи DDR1, DDR2 і FB-DIMM, що використовуються в ТЛКО, з усією переконливістю продемонструвало таке:

вплив збоїв (відмов) в оперативній пам'яті телекомунікаційного обладнання істотно недооцінюється;

збої (відмови) оперативної пам'яті виникають набагато частіше, ніж до цього було прийнято вважати;

багато допущень, наприклад, що оперативна пам'ять практично не "старіє", як "старіють", підвищуючи ймовірність відмов, компоненти з рухомими частинами (такі, наприклад, як жорсткі диски), або що перегрів згубно позначається на роботі ОЗП, є невірними і вимагають перегляду [16].

Дослідження показало, що приблизно кожен третій сервер (або 8 % модулів пам'яті) у спостережуваних датацентрах протягом 2,5 року дослідження зустрічався зі збоєм в оперативній пам'яті. Було встановлено, що число збоїв, зареєстрованих системою моніторингу, майже в п'ятнадцять разів перевищує більш ранню оцінку і складає понад 4 000 на рік. Велика частина з них була усунена з використанням коригувальних кодів (ECC, Error Correction Code) і більш складними його

варіантами, такими як Chipkill (дозволяє усунути багатобітові помилки, наприклад, відразу в групі комірок). Тим не менш, є помилки, які не вдалося виправити (невиправна помилка, (Uncorrectable Errors), і які призвели до відмов (критична системна помилка (BSOD, Blue Screen of Death), критична помилка ядра операційної системи (kernel panic) зустрічаються куди частіше, ніж це прийнято вважати (1,3 % серверів в рік або близько 0,22 % в оперативній пам'яті). У разі використання пам'яті без ECC кожна з таких помилок призводить до відмов у роботі програми. Адже, наприклад, дуже багато користувачів зберігають дані баз в пам'яті для прискорення її роботи. Було встановлено, що ймовірність отримати повторний збій у модулі пам'яті, що вже раніше давав збій, у сотні разів вища, у порівнянні з тим, в якому раніше не виникав збій. Це може бути викликано як наявністю технологічного браку, який погано виявляється, так і тим, що відмова, наприклад пробій зарядженою часткою космічних променів, не проходить для пам'яті безслідно, навіть якщо помилка була скоригована ECC. У 70–80 % випадках, коли реєструвалася відмова (невиправна помилка) у модулі пам'яті, цей модуль уже мав збій.

Нарешті, був продемонстрований ефект "старіння" в модулях оперативної пам'яті (DRAM). Більш того, у пам'яті він проявився куди більш явно, ніж, наприклад, у жорстких дисках (HDD), де поріг, після якого відмови зростають у рази, становив приблизно 3–4 роки.

Парадоксальним чином статистика демонструє збільшення темпу зростання збоїв (коректованих помилок) зі збільшенням віку модулів, але знижується темп для відмов (некоректованих помилок), проте швидше за все це просто результат планової заміни пам'яті в серверах, які були помічені зі збоями.

Модулі оперативної пам'яті (DRAM), позбавлені будь-яких рухомих частин, показують істотне і тривале зростання збоїв уже після року-півтора експлуатації. Наприклад, спостереження за десятками тисяч серверів Google, що проводилися протягом двох з половиною років, показали, що частота помилок у модулях пам'яті перевищує в сотні і тисячі разів загальноприйняті уявлення про можливу інтен-

сивність збоїв даного типу. У середньому на один модуль оперативної пам'яті припадає 3751 збоїв (коректованих помилок) протягом року.

Аналіз показав, що в оцінці показників надійності сучасних мереж зв'язку необхідно враховувати не тільки стійки відмови, а і збої у роботі протоколів маршрутизації та у програмному забезпеченні телекомунікаційного обладнання.

Напрямом подальших досліджень є розробка вдосконаленого науково-методичного апарату для комплексної оцінки надійності телекомунікаційного обладнання мережі зв'язку з урахуванням збоїв і відмов.

Список використаної літератури

1. W. Ahmada Reliability modeling and analysis of communication networks / W. Ahmada, U. Pervez, J. Qadirb. // Journal of Network and Computer Applications. – V.78. – 15 January. – 2017, P. 191–215.

2. V. Devis Dependability in Future Battle Network System – Transport Layer Ability to Maintain Quality of Service / V. Devis // Center for Applied Research, Estonian National Defence College, Tartu, Estonia. – 2016. – P. 211–228.

3. Нетес В. А. Надежность сетей связи в период перехода к NGN / В. А. Нетес // Вестник связи. – 2007. – № 9. – С. 126–130.

4. Norros I. A broad approach to the dependability of IP networks / Norros I. // European CUP Newsletter. – 2006. – Vol. 2. – №. 3. – P. 12 – 23.

5. Парфенов Б. А. NGN-проблемы / Б. А. Парфенов // Вестник связи. – 2006. – № 12 – С. 54–56.

6. Гольдштейн Б. С. 10 лет эволюции коммутационной техники / Б. С. Гольдштейн // Вестник связи. – 2007. – № 5. – С. 22–30.

7. Norros I. Abroad approach to the dependability of IP networks // European CUP Newsletter. – 2006. –Vol. 2. – № 3. – P. 24–29.

8. Нетес В.А. Уроки Интернета / В. А. Нетес // Вестник связи. – 2006. – № 4. – С. 62–68.

9. Next Generation Networks Task Force Report // The President's National Security Telecommunications Advisory Committee. March 28, 2006.

10. Duffy J. Cisco routers caused major outage in Japan: report / Duffy J. // Network World 16.05. – 2007. – P. 1 –20.

11. Дроботун Е. Б. Критичность ошибок в программном обеспечении / Е. Б. Дроботун // Фундаментальние исследования. – 2009. – № 4. – С. 73–74.

12. ДСТУ 2860–94. Надійність техніки. Терміни та визначення. Чинний від 1996–01–01. – К. : Держстандарт України, 1994. – 90 с.

13. Попсулин С. Сбои GPS длительностью 13 микросекунд вызвал многочасовые глобальные проблемы – Телеком Техника [Электронный ресурс]. – Режим доступа : http: //m.cnews.ru/news/top/2016-02-05

14. Стеклов В. К. Телекомунікаційні мережі : підручник / В. К. Стеклов, Л. М. Беркман. – К. : Техніка, 2001. – 392 с.

15. Pinhero E. DRAM Erors in the Wild: A Large-Scale Field Study / Sigmetrics // Performance, Jyne 15–19, 2009. – P. 34–46.

16. Статистика отказов в серверной памяти / DeadLock-Habrahabr [Электронный ресурс]. – Режим доступа : https: // m.habrahabr.u/post/171407/

Рецензент – доктор технічних наук, професор Могилевич Д. І.

Кононова И. **Анализ влияния сбоев на надежность телекоммуникационного оборудования сетей связи**

Проведен анализ влияния сбоев на надежность телекоммуникационного оборудования сетей связи. Показано, что игнорирование сбоев программного обеспечения телекоммуникационного оборудования может привести к существенным потерям временных и человеческих ресурсов. Поэтому при оценке показателей надежности современных сетей связи необходимо учитывать сбои в работе протоколов маршрутизации и в программном обеспечении телекоммуникационного оборудования.

Ключевые слова: *сеть связи, показатели надежности,протоколы маршрутизации, отказ, сбой.*

Kononova I. **Analysis of effects of suspending on reliability telecommunication equipment communication network**

Until now, most specialists of telecommunication networks formed the idea of inappropriate conduct of scientific research and use of practical measures related to quantitative assessment and ensuring the stability of this class of technically sophisticated systems. But the analysis showed that neglect to ensure reliability of telecommunication equipment of modern communication networks can lead to significant loss of time and human resources. Using of new technologies in communication networks, as well as

telecommunication equipment, in which microprocessor elements, memory and software are widely used, has led to the emergence of a new source of failures - errors in the operation of routing protocols and in the software of the equipment itself. Routing protocols are sensitive to configuration errors and because of the peculiarities of their work such violations can spread in communication networks as an avalanche. Errors in the software of telecommunication equipment are also significant and affect the reliability of the network as a whole. The main reasons that cause a disruption of normal functioning programs, there are errors that are hidden in the program itself; distortion of incoming information to be processed; wrong user's actions. For any telecommunication equipment there is an allowable time of absence of data from the program, in which its characteristics are within the permissible limits .Based on this time, we can set the boundaries of the time, which separates the active and inactive state of the software and allows you to use these boundaries as a criterion for failures (errors of functioning).In the work, is shown assessment of the impact of failures on reliability of telecommunication equipment of communication networks. It is shown the necessity of taken comprehensive consideration when assessing the reliability of modern networks communication, errors in the operation of routing protocols and in the software, provision of telecommunication equipment. The direction of further research is the development of an advanced scientific and methodical apparatus for comprehensive assessment of the reliability of the telecommunication equipment of the communication network, taking into account errors and failures.

Keywords: *communication network, reliability indicators, routing protocols, refusal, error.*