К. П. Сторчак, Т. П. Довженко
ДОСЛІДЖЕННЯ МЕРЕЖІ TCP/IP З ВИКОРИСТАННЯМ ПРОГРАМНОГО КАРКАСУ ERLANG/OTP
Розглянуто програмний каркас (фреймворк) Erlang/OTP і проведено дослідження мережі TCP/IP із застосуванням цього фреймворка.
Ключові слова: Erlang/OTP; RED; PI; AQM; алгоритм активного управління чергою; TCP/IP-протокол.

K. Storchak, T. Dovzhenko
RESEARCH OF TCP/IP NETWORK USING THE ERLANG/OTP FRAMEWORK
In this article considered a software framework (framework) Erlang / OTP and investigated TCP/IP network using the framework.
Keywords: Erlang/OTP; RED; PI; AQM; active queue management algorithm; TCP/IP-protocol.

УДК 004.738

С. І. ОТРОХ, канд. техн. наук, доцент;
В. О. ЯРОШ, аспірант;
Є. П. ГОРОХОВСЬКИЙ, здобувач;
Ю. М. ЗІНЕНКО, здобувач,
Державний університет телекомунікацій, Київ

Оцінювання показників стійкості мережі майбутнього (FN) до зовнішніх дестабілізуючих факторів

Подано визначення мережі майбутнього (FN), головна відмітна особливість якої — це здатність до самовідновлення та самоорганізації завдяки притаманній сталості та стійкості до дії стихійних лих. Сформовано методи забезпечення стійкості мережі та її відновлення після впливу стихії. Розроблено систему оцінювання показників стійкості до потужного електромагнітного та іонізуючого випромінювання, а також подано рекомендації стосовно підвищення стійкості мереж FN до дії зовнішніх дестабілізуючих факторів.

Ключові слова: мережі майбутнього; стихійні лиха; зовнішні дестабілізуючі фактори; стійкість.

Вступ

У наш час, коли людство потерпає від небачених досі катастроф техногенного та природного характеру, посилюються загрози локальних конфліктів, дедалі важливішого значення набуває завдання забезпечити стале функціонування мережі майбутнього (**FN** — *Future Networks*) — результат еволюційного розвитку мереж наступного покоління [1]. Концепція FN характеризується безперервною зміною вимог до телекомунікаційних мереж, появою принципово нових прикладних сфер дистанційного керування побутовою та іншою технікою (Internet of Things), створенням «розумних» мереж (Smart Gridg) із використанням хмарних обчислень (Cloud Computing).

Згідно з визначенням МСЕ, мережа майбутнього [2] являє собою глобальну інформаційну інфраструктуру, яка включає в себе наявні інформаційно-комунікаційні мережі з урахуванням тих компонентів, які тільки плануються до впровадження. Єдиним центром управління глобальною інформаційною інфраструктурою забезпечується здатність надавати повний спектр телекомунікаційних послуг (у будь-якому географічному районі, причому гарантованої якості, прийнятної вартості та в будь-який час) на базі новітніх та інноваційних технологій. Головна істотна характеристика FN полягає в її здатності до самовідновлення та самоорганізації за рахунок сталості та стійкості до дії стихійних лих. Безвідмовне функціонування FN під час дії стихійного лиха — це чинник забезпечення потреб щодо управління державою, підтримання її обороноздатності, гарантування безпеки, охорони правопорядку, господарського комплексу країни, а також потреб фізичних і юридичних осіб щодо високоякісних послуг телекомунікацій.

Отже, в епоху глобальних змін, передбачуваних і непередбачуваних загроз необхідно сформувати такі вимоги до FN, щоб вона не втрачала стійкості під впливом будь-яких зовнішніх дестабілізуючих факторів (ЗДФ). Для того, аби якомога надійніше захистити мережу, необхідно розробити певні рекомендації стосовно проектування FN із метою мінімізації дії ЗДФ та відновлення сталого функціонування мережі. ЗДФ — це певний вид зовнішніх впливів, параметри якого перевищують ті значення, на які було розраховано елемент мережі при його проектуванні. До ЗДФ віднесено також стихійні лиха, про які йдеться в Рекомендації L.392 сектору стандартизації Міжнародного союзу електрозв'язку, поданій наприкінці 2016 року [3].

Основна частина

Стійкість мережі та її відновлення після дії стихійного лиха досягаються за допомогою багатократних методів [3]. *Головний метод* передбачає ***максимальне посилення*** (*укріплення*) ***мереж***,

стійких до дії ЗДФ, для мінімізації потенційних збитків. Суть цього методу полягає в резервуванні, резервному копіюванні та перемиканні системи або її частини. *Вторинний метод* полягає в ***забезпеченні розгортання устаткування на відновлюваних об'єктах*** для належного функціонування FN та надання послуг зв'язку після дії ЗДФ. Коли стихійне лихо мине, потрібно негайно розгорнути ці підготовлені ресурси на пошкоджених ділянках. Цей метод добре працює, коли мережні об'єкти, захищені завдяки застосуванню головного методу, виходять із ладу або руйнуються. Зазначені методи вдало доповнюють один одного.

Згідно з [4] типові стихійні лиха систематизовано у вигляді наведеної далі таблиці.

Типові стихійні лиха

№ з/п	Стихійні лиха	Наслідки	Можливі запобіжні заходи
1	Землетруси	Пошкодження всіх зовнішніх об'єктів телекомунікацій, розриви ліній зв'язку	Формування максимально жорстких вимог до будівельних норм і норм проектування, які забезпечать високу опірність споруд до землетрусу. Уникнення наявності встановленого обладнання в найімовірніших зонах землетрусу. Використання якомога міцніших матеріалів при побудові зовнішніх об'єктів телекомунікацій. Використання гумових з'єднань для лінійно-кабельної інфраструктури та збільшення кількості волоконно-оптичного кабелю в колодязях кабельної каналізації з метою недопущення розривів при зміщенні земної кори. Проведення імітаційного сейсмічного моделювання з метою вчасного попередження про можливий землетрус. Упровадження вібраційного контролю та створення системи моніторингу мережі
2	Цунамі	Пошкодження всіх зовнішніх об'єктів телекомунікацій, руйнування систем енергозабезпечення	Побудова об'єктів телекомунікацій та лінійно-кабельних споруд на узвиші. Побудова мережі з використанням переважно кільцевої топології для уможливлення доступу об'єкта телекомунікацій у двох рознесених між собою географічних напрямах. Прокладання кабелів у трубопроводах по руслу річки, а не по мостах. Забезпечення об'єктів телекомунікацій електроживленням завдяки створенню двох чи кількох незалежних маршрутів електроживлення.
3	Надсильні повені	Заводнення кабельних каналізацій, потенційне пошкодження кабелів	Обмеження побудови об'єктів телекомунікацій у зонах можливого затоплення. Використання залізобетонних конструкцій на ділянках, де існує велика ймовірність затоплення. Створення огорожі, що забезпечить захист об'єктів телекомунікацій від затоплення; встановлення водонепроникних дверей і водяних насосів
4	Лісові пожежі	Пошкодження підвісних кабелів зв'язку та зовнішніх об'єктів телекомунікацій, розташованих у лісовій місцевості	Розміщення об'єктів телекомунікацій поза зоною лісового масиву або в підземних спорудах
5	Урагани/ торнадо/ тайфуни	Руйнування телекомунікаційних щогл чи веж, пошкодження підвісних кабелів зв'язку	Формування якомога жорсткіших вимог до будівельних норм і норм проектування для захисту об'єктів телекомунікацій від сильних вітрів. Установлення допоміжних розпірок між стовпами у вітряних місцях, де можлива швидкість вітру понад 40 м/с. Використання віброгасників для захисту підвісних кабелів зв'язку
6	Зсуви грунту	Руйнування кабелів, закладених у грунт, пошкодження лінійно-кабельної інфраструктури	Обмеження щодо встановлення телекомунікаційного обладнання в зонах із високою ймовірністю зсуву грунту. Укріплення схилів. Установлення систем моніторингу та контролю за зсувом грунту
7	Надсильний холод/ надсильна спека	Руйнування телекомунікаційного обладнання	По змозі розміщення об'єктів телекомунікацій у підземних спорудах
8	Надвисока сонячна активність та потужне електромагнітне випромінювання	Повне знищення телекомунікаційного обладнання	По змозі розміщення об'єктів телекомунікацій у підземних спорудах. Формування якомога жорсткіших вимог до будівельних норм та норм проектування для підвищення опірності споруд та потужного електромагнітного випромінювання

Щоб запобігти наслідкам, до яких можуть призвести катастрофи техногенного та природного характеру, необхідно розробити план боротьби зі стихійними лихами, який має включати в себе такі заходи.

• *Профілактика* — види діяльності, які фактично усувають або зменшують імовірність катастрофи.

• *Готовність* — діяльність, здійснювана для запобігання стихійним лихам, реагування на них та ліквідації можливих наслідків. На цьому етапі розробляються заходи, які допоможуть врятувати життя людей і мінімізувати збитки від дії лих (наприклад, установлення систем раннього попередження).

• *Відповідь* — діяльність після стихійного лиха. Ці заходи мають стабілізувати ситуацію та зменшити ймовірність вторинного ушкодження.

• *Відновлення* — заходи, необхідні для повернення всіх систем до нормального функціонування (наприклад, відновлення знищеного майна або ремонт необхідної інфраструктури).

Сьогодні на території України поява ЗДФ 1–7 малоймовірна. Натомість надвисока сонячна активність, іонізація космічного простору та потужне електромагнітне випромінювання — чинники особливо актуальні. Як показують дослідження, сукупність зовнішніх чинників природного характеру за певних умов впливає на роботоздатність FN, що призводить до спотворення інформації або

її повної втрати. Ще до більш негативного впливу на роботоздатність засобів зв'язку призводять такі зовнішні чинники природного чи штучного характеру, як іонізуюче випромінювання (ІВ) та потужне електромагнітне випромінювання (ЕМВ). Основними джерелами таких випромінювань виступають надвисока сонячна активність, блискавки тощо [5]. Дія ІВ та ЕМВ може суттєво змінювати характеристики елементів FM, викликати серйозні, навіть необоротні порушення роботоздатності мережі. Отже, одне з актуальних завдань полягає в побудові такої FN, що буде стійка до різних видів ЗДФ природного та штучного характеру.

Зауважимо, що ЕМВ та ІВ — це надвисоке рентгенівське й гамма-випромінювання, а також світлове (теплове) випромінювання та електромагнітний імпульс унаслідок дії надвисокої сонячної активності.

Аналізуючи зміни параметрів елементів під впливом потоку нейтронів, бачимо, що вибір показника стійкості елемента деякої FN неможливо здійснити однозначно. Це пов'язано з умовністю вибору такого рівня зміни параметра, який вважається характеристикою «граничного стану» елемента, використовуваного в тій чи іншій FN.

Як показники, що характеризують стійкість елемента FN, можна взяти [5]:

1) ***початкову стійкість*** $\boldsymbol{R_{i\text{поч}}}$ — максимальне значення характеристик ІВ та ЕМВ (потік нейтронів, гамма-випромінювання, електронне та протонне випромінювання, тобто потужність дози, за якої жодний із параметрів i-го комплектуючого елемента ще не зазнає змін;

2) ***технічну стійкість*** $\boldsymbol{R_{i\text{ТС}}}$ — значення характеристик випромінювання, які вказано в документації i-го елемента;

3) ***допустиму стійкість*** $\boldsymbol{R_{i\text{доп}}}$ — максимальне значення характеристик випромінювання, за яких параметри FN ще перебувають у межах, встановлених технічною документацією на цю мережу;

4) ***граничну стійкість*** $\boldsymbol{R_{i\text{гр}}}$ — значення характеристик випромінювання, вказані в технічній документації на елемент FN як його гранична радіаційна стійкість.

Зауважимо, що $R_{i\text{поч}}$ знаходять за графіком математичного сподівання зміни параметра комплектуючого елемента як функції (наприклад, від потоку нейтронів), визначаючи точку, починаючи з якої відбувається реєстрована зміна розглядуваного параметра. Потік нейтронів, що відповідає цій точці, беруть як $R_{i\text{поч}}$.

При визначенні інших показників стійкості необхідно брати до уваги статистичний розкид показників стійкості від зразка до зразка в партії ЕМВ. Цей чинник враховується переходом від кількісних показників, визначених за залежностями середніх значень відповідних параметрів від рівня радіаційного чинника, до показників, які характеризують рівень радіаційного чинника, який відповідає зміні параметра, узятого як критерій відмови елемента. При цьому для врахування можливого розкиду показників стійкості від елемента до елемента є сенс брати за показники стійкості нижні межі толерантних інтервалів, які з імовірністю γ гарантують потрібні частки P (у відсотках) сукупності елементів розглядуваного типу.

Нижні толерантні межі для показників такі [5]:

$$R^{*} = \overline{R}_i - KS_{R_i}, \qquad (1)$$

де $\overline{R}_i$ — значення показників стійкості, визначені за середнім значенням зміни параметра елемента залежно від потоку (дози); K — коефіцієнт, залежний від обсягу n вибірки, за результатами випробувань якої отримано дані щодо стійкості ЕМВ, а також вибрані (задані) значення γ і P;

$$S_{R_i} = \frac{\overline{R}_i S_{q_i}\left(\overline{R}_i\right)}{m_{q_i}\left(\overline{R}_i\right)} \qquad (2)$$

— середньоквадратичне відхилення потоку (дози), визначене з напівемпіричної формули; $S\left(\overline{R}_i\right)$ — середньоквадратичне відхилення параметра в точці, яка відповідає значенню $\overline{R}_i$; $m_{q_i}\left(\overline{R}_i\right)$ — середнє значення параметра в точці, яка відповідає значенню $\overline{R}_i$.

При визначенні кількісних показників стійкості до впливу нейтронного потоку необхідно враховувати, стосовно якого (імпульсного чи неперервного) впливу задано вимоги щодо стійкості на апаратуру, а також на яких (імпульсних чи неперервних) реакторах отримано наявні данні про стійкість комплектуючих елементів.

Такі міркування правомірні в разі, коли імпульсний потік нейтронів $\Phi_{i\,\text{ім}}$, що характеризує стійкість i-го елемента, задано за допомогою співвідношення

$$\Phi_{i\,\text{ім}} = \kappa_{\text{еф}\,n}(\Phi_i), \qquad (3)$$

де Φ_i — потік нейтронів (характеризує стійкість елемента), отриманий у будь-якому джерелі випромінювання; $\kappa_{\text{еф}\,n}$ — коефіцієнт ефективності джерела нейтронного випромінювання.

Отже, стійкість FN до дії зовнішніх дестабілізуючих факторів забезпечується:

- вибором типу споруд об'єктів зв'язку, які зазнають безпосереднього впливу потужних гармонічних електромагнітних полів, електромагнітних імпульсних полів блискавки та іонізуючого випромінювання;
- засобами захисту обладнання систем передавання мережі зв'язку від безпосереднього впливу електромагнітних полів;
- вибором типу кабелів та параметрів їх прокладання, а також міжстоякових з'єднань обладнання зв'язку на об'єктах кабельних систем передавання;

• підвищенням стійкості обладнання на об'єктах кабельних систем передавання до взаємодії електромагнітних полів;

• захистом обладнання зв'язку на об'єктах кабельної інфраструктури від комплексної взаємодії електромагнітних полів та іонізуючого випромінювання.

Згідно зі сказаним розроблено рекомендації щодо підвищення стійкості FN до дії ЗДФ, наведені на рисунку.

Висновок

Запропоновано методи забезпечення стійкості FN та її відновлення після дії стихійного лиха.

Методи підвищення стійкості FN до дії ЗДФ

Список використаної літератури

1. ***Нетудихата, Л. І.*** *Телекомунікаційні мережі майбутнього (Future networks) як еволюційний розвиток мережі наступного покоління (Next Generation Network) / Л. І. Нетудихата, В. Б. Каток, С. І. Отрох // Зв'язок.— 2011.— № 3.— С. 2–4.*

2. ***Global*** *information infrastructure, internet protocol aspects and Next Generation Networks — future networks. Future Networks: Objectives and Design Goals // Recommendation ITU-T Y.3001.— 2011.*

3. ***Disaster*** *management for improving network resilience and recovery with movable and deployable information and communication technology (ICT) resource unit // Recommendation ITU-T L.392.— 2016.*

4. ***Rec. ITU-TL.92.*** *Disaster management for outside plant facilities.— 2012.*

5. ***Мырова, Л. О.*** *Обеспечение стойкости аппаратуры связи к ионизирующим и электромагнитным излучениям / Л. О. Мырова, А. З. Чепиженко.— Радио и связь.— М., 1988.— 296 с.*

Рецензент: доктор техн. наук, професор **Л. Н. Беркман**, Державний університет телекомунікацій, Київ.

С. И. Отрох, В. А. Ярош, С. П. Гороховский, Ю. Н. Зиненко

ОЦЕНКА ПОКАЗАТЕЛЕЙ УСТОЙЧИВОСТИ СЕТИ БУДУЩЕГО (FN) К ВНЕШНИМ ДЕСТАБИЛИЗИРУЮЩИМ ФАКТОРАМ

Приведено определение сети будущего (FN), главной отличительной особенностью которой является способность к самовосстановлению и самоорганизации благодаря ее постоянству и устойчивости к воздействию стихийных бедствий. Сформированы методы обеспечения устойчивости сети и ее восстановления после воздействия стихии. Разработана система оценки показателей устойчивости к мощному электромагнитному и ионизирующему излучению, а также даны рекомендации по повышению устойчивости FN к воздействию внешних дестабилизирующих факторов.

Ключевые слова: сети будущего; стихийные бедствия; внешние дестабилизирующие факторы; устойчивость.

S. Otroh, V. Yarosh, E. Gorohovskyy, Yu. Zinenko

EVALUATION OF RESISTANCE TO DESTABILIZING EXTERNAL FACTORS FUTURE NETWORK (FN)

The definition of the future network is considered in the article and its main difference in ability to heal itself and self-organization due to its permanence and resistance to natural disasters is proved. The methods of sustaining the network and its recovery after exposure to disasters are formed. The assessment of resistance to electromagnetic and ionizing radiation of ultra-high solar activity and recommendations to increase the resilience of future networks to EDF action is developed.

Keywords: future networks; natural disasters; external destabilizing factors (EDF); stability.