РАДІОТЕХНІКА, ЕЛЕКТРОНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

УДК 004.891

Д.О. ЯРОЩУК, О.А. МЯСИЩЕВ
Хмельницький національний університет

УДОСКОНАЛЕННЯ МЕТОДУ ОБРАХУНКУ ВПЛИВУ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ЕФЕКТИВНІСТЬ ФУНКЦІОНУВАННЯ ЗАКРИТОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Розглядається завдання забезпечення ефективного функціонування телекомунікаційних мереж (ТКМ). Від того як функціонують ТКМ установи залежать критичні аспекти його діяльності. Найперспективнішим напрямком розвитку закритих мереж є перехід від орендованих каналів зв'язку до відкритих каналів мережі Інтернет. Однак використання відкритих Інтернет мереж призводить до загроз інформаційної безпеки. Розроблені методи оцінки захищеності об'єктів мережі від загроз інформаційної безпеки засновані на якісній експертній оцінці. Проведено удосконалення в переході до кількісної оцінки ефективності функціонування ТКМ на підставі критеріїв доступності інформації і послуг зв'язку.

Ключові слова: телекомунікаційна мережа, інформаційна безпека, ефективність, оцінка.

D.A. YAROSCHUK A.A. MYASISCHEV
Khmelnytsky National University

IMPROVING OF THE METHOD OF INFLUENCE OF INFRINGEMENT OF INFORMATION SECURITY ON THE EFFICIENCY OF FUNCTIONING OF CLOSED TELECOMMUNICATION NETWORK

The article deals with the task of ensuring the efficient functioning of telecommunication networks. From the functioning of the telecommunications network of the closed network of the educational institution, the critical aspects of its activity depend, the task of ensuring the effective functioning of the network is extremely acute. The most promising direction of the development of corporate networks that can meet the growing needs of private networks is the transition from using their own or leased communication channels to open, built with the use of the Internet or other networks. However, the use of open Internet networks is accompanied by the fact that they are exposed to the impact of specific for open telecommunication networks threats to information security, which affects their performance. The methods of assessing the security of network objects from threats of information security developed to this moment are based on qualitative expert evaluation. Their improvement is offered in the part of the transition to a quantitative assessment of the efficiency of telecommunication networks functioning on the basis of the criteria for the availability of information and communication services. Mathematical modelling, as well as natural experiments and statistical research methods are used to solve the problems. Experimental verification was carried out by conducting field experiments, using hardware and software used on communication nodes of the investigated network. The proposed method allows to evaluate the efficiency of the functioning of the corporate telecommunication network with the formation of the result of evaluation in the form of a quantitative indicator, thereby increasing the quality of the assessment. The software developed during the study is designed to quantify the performance of the network elements. As a result of this analysis, it is possible to use the mathematical and methodical apparatus of the theory of reliability for the analysis of the structural reliability of complex telecommunication networks. As an indicator of the efficiency of functioning of networks and their elements, Kg is chosen as the normalized reliability index of telecommunication networks and their elements. Thus, the possibility of increasing the efficiency of network operation by topological methods is substantiated.

Keywords: telecommunication network, information security, efficiency, evaluation.

Вступ. В умовах, коли системи зв'язку життєво необхідні для нормального функціонування організації, вони стають пріоритетною метою для зловмисників. Шляхом впливу на телекомунікаційну мережу (ТКМ) можливо організувати атаки, що реалізують загрози, спрямовані на всі три основні властивості інформації. Загроза безпеки інформації – це сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення безпеки інформації. При реалізації загроз інформаційної безпеки (ІБ) виникає небезпека знищення, перекручення, блокування, копіювання, поширення інформації, а також інших несанкціонованих дій з нею.

Незалежно від конкретних видів загроз ІБ, що впливають на досліджувану інформаційну систему, потрібно забезпечити такі основні властивості автоматизованої системи та інформації в якій циркулюють: цілісність, конфіденційність і доступність. Конфіденційність інформації - це стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на нього право. Цілісність інформації – це стан інформації, при якому її зміна здійснюється тільки навмисно суб'єктами, що мають на нього право. Доступність інформації – це стан інформації, при якому суб'єкти, які мають право доступу, можуть реалізувати його безперешкодно. На момент проведення дослідження завдання захисту переданої по ТКМ інформації від загроз цілісності і конфіденційності успішно вирішується застосуванням засобів криптографічного захисту інформації. У той же час загальне застосування рішення задачі забезпечення доступності інформації в ТКМ на момент проведення дослідження нам невідомо. В даному дослідженні під загрозою доступності інформації розуміються загрози ІБ, спрямовані на порушення доступності інформації. У даній роботі буде розроблений метод дослідження ТКМ, застосування якого дозволяє оцінити ефективність функціонування ТКМ в умовах впливу загроз доступності інформації. Таким чином, на основі дослідження, що враховує вплив загроз доступності інформації, стає можливим провести заходи, спрямовані на їх нейтралізацію та оцінити ефективність цих захисних заходів.

В даний час питаннями забезпечення і підвищення ефективності функціонування ТКМ займається досить велика кількість наукових колективів, провідні розробники з різних напрямків по всьому світі. Дослідником, що сформулював загальні вимоги до розробки відмовостійких систем, чиї праці лягли в основу багатьох перспективних розробок, є A. Avizienis, в дослідженнях якого (зокрема), визначено взаємозв'язок між надійністю обчислювальних систем і їх ІБ, а також розроблені підходи до забезпечення ІБ з боку забезпечення відмовостійкості.

Для вирішення завдання визначення показників надійності великих об'єктів, що складаються з безлічі різнорідних елементів, таких як ТКМ, використовується підхід їх моделювання у вигляді марківських процесів. Такий підхід є певним спрощенням в порівнянні з реальними процесами, що відбуваються в елементах ТКМ. У даній роботі використаний аналогічний підхід з вибором об'єкта дослідження у вигляді елементів ТКМ.

На сьогоднішній день розвиток інформаційних технологій і ТКМ призвело до того, що при побудові корпоративних інформаційних систем (ІС) в організаціях використовуються ТКМ загального користування (відкриті ТКМ). Використання мереж загального користування дозволяє організації заощадити значні кошти на оренду або побудові власної мережевої інфраструктури. Однак передача інформації за відкритими ТКМ несе в собі значні ризики, спрямовані на всі основні властивості інформації: цілісність, конфіденційність і доступність. Оцінка захищеності від загрози цілісності і конфіденційності на сьогоднішній день базується на превентивні заходи криптографічного захисту інформації. Однак загрози доступності інформації є специфічними для відкритих ТКМ, і на сьогоднішній день не існує єдиної методики їх оцінки. Найбільш поширені різні методики експертної оцінки ІБ, проте їх використання не може забезпечити формування цілісної об'єктивної картини.

Таким чином, використання єдиної методики, що включає в себе облік впливу як технічних характеристик ТКМ, так і їх захищеність від специфічних загроз ІБ, дозволить значно підвищити ефективність проектування захищених корпоративних ІС, оскільки одним з найважливіших показників при їх проектуванні є захист від загроз ІБ, в зокрема - забезпечення доступності циркулюючої в ІС інформації. Удосконалення методу оцінки та підвищення ефективності функціонування ТКМ є актуальним і затребуваним завданням.

Постановка задачі. Провести аналіз факторів, що впливають на забезпечення ефективного функціонування ТКМ, критеріїв та існуючих методів оцінки ефективності функціонування ТКМ. Визначити фактори, що впливають на ефективність функціонування ТКМ з боку загроз ІБ. Проаналізувати можливість застосування методичного та математичного апарату теорії надійності як методу дослідження ТКМ для оцінки впливу загроз ІБ на забезпечення ефективного функціонування ТКМ. Проаналізувати можливість підвищення ефективності функціонування вузлів зв'язку ТКМ шляхом вдосконалення їх мережевих топологій (топологічними засобами).

Основна частина. На ефективність функціонування ТКМ в першу чергу впливає працездатність елементів ТКМ. Для елементів ТКМ розрізняють 2 основних стани технічних пристроїв: працездатна і непрацездатна. Під працездатним станом розуміється стан виробу, при якому воно здатне виконувати необхідну функцію за умови надання необхідних зовнішніх ресурсів. Під непрацездатним станом - стан, при якому виріб не здатний виконувати необхідне завдання з будь-якої причини. Причини непрацездатності можуть мати різну природу, при цьому існують різні підходи до їх класифікації. Адаптована для ТКМ версія класифікації зображена на рис. 1.

На рис. 1 представлена діаграма причин відмов елементів ТКМ. У червоному секторі згруповані первинні відмови елемента, причиною яких є елемент сам по собі. Причини первинних відмов можуть бути обумовлені як недосконалістю технологічних процесів при виробництві елемента (заводським дефектом), так і природним старінням елементів по закінченню рекомендованого періоду експлуатації. У синьому секторі згруповані вторинні відмови елементів. Причиною вторинного відмови є не елемент сам по собі, а якісь зовнішні чинники. Ними можуть бути неякісні зовнішні ресурси, необхідні для нормального функціонування елемента – вихід параметрів навколишнього середовища за межі, передбачені виробником обладнання, проблеми пов'язані з електроживленням обладнання, пошкодження, викликані виходом з ладу сусідніх елементів, інженерно пов'язаних з ними. У зеленому секторі згруповані відмови, викликані людським фактором і неправильною експлуатацією обладнання. Переважно до них відносяться неправильні команди персоналу. Незважаючи на те, що в кінцевому підсумку наслідком будь-якої з перерахованих вище причин є порушення працездатності елемента ТКМ, відмови з різними причинами їх виникнення враховуються в показниках надійності по-різному.

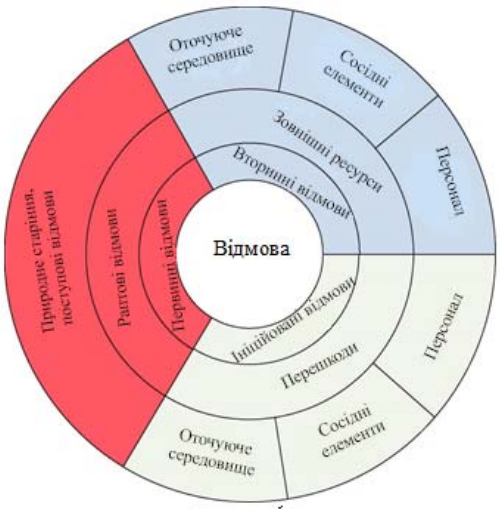

Рис. 1. Діаграма відмов елементів ТКМ

Для визначення захищеності ТКМ необхідно розробити математичну модель стану її елементів, на підставі якої можна здійснити прогнозування її станів. Таким чином, необхідно визначитись з набором станів, в яких можуть знаходитися елементи досліджуваної системи, і визначити причини, що викликають переходи між ними. Також необхідно визначити ступінь впливу стану елементів, що складають ТКМ, на стан ТКМ в цілому. Також необхідно визначити метод розрахунку, за допомогою якого здійснюється розрахунок характеристик ТКМ в цілому через характеристики її елементів.

Кожен елемент ТКМ являє собою сукупність певних технічних пристроїв (обладнання). Устаткування елемента ТКМ є відновлювані об'єкти. На рисунку 2 представлений граф станів обладнання, де першому відповідає справний стан об'єкта, другому несправний стан, А. – інтенсивність потоку відмов, μ – інтенсивність потоку відновлень.

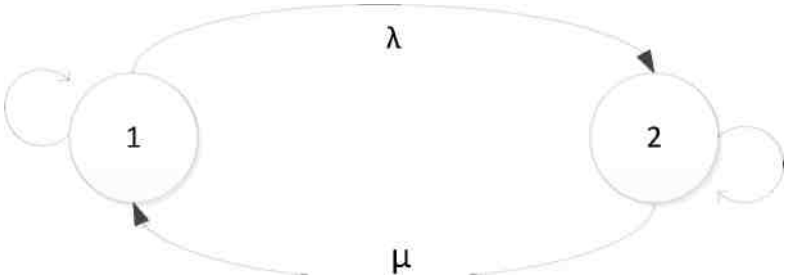

Рис. 2. Граф станів обладнання елемента ТКМ

Коли стан обладнання стабілізовано (воно знаходиться або в справному, або в несправному стані), його поведінку можна прирівняти до поведінки невідновлюваного об'єкта. При виключенні з розгляду часу відновлення пристрою (оскільки в цей час відмова статися не може) відмови формують потік. Відповідно інтенсивність потоку відмов буде розраховуватися за формулою (1):

$$\lambda(t) = \frac{n(t)}{N_{cp} \times \Delta t}, \tag{1}$$

де $n(t)$ – число пристроїв, що знаходяться в непрацездатному стані на інтервалі часу Δt,

Δt – інтервал часу,

N_{cp} – середнє число пристроїв, що знаходяться в працездатному стані на інтервалі часу Δt.

Також інтенсивність потоку відмов можна виразити за допомогою (2) ймовірності безвідмовної роботи і частоти відмов:

$$\lambda(t) = \frac{N_0 \times a(t)}{N_{cp}(t)}, \tag{2}$$

де N_0 – число пристроїв, що знаходяться в працездатному стані на момент початку спостереження,

$a(t)$ – середньостатистична ймовірність знаходження пристрою в непрацездатному стані.

Середньостатистична ймовірність знаходження пристрою в непрацездатному стані визначається за (3):

$$a(\Delta t) = \frac{N(\Delta t) \times \overline{tв}}{N_0 \times \Delta t}, \tag{3}$$

де $N(\Delta t)$ – число пристроїв, що знаходяться в непрацездатному стані в інтервалі часу Δt,

$\overline{tв}$ – середньостатистичний час знаходження пристрою в непрацездатному стані,

N_0 – число пристроїв, що знаходяться в працездатному стані на момент початку спостереження,

Δt – інтервал часу.

Оскільки відмови пристроїв є випадковими подіями і підкоряються експоненціальним законом розподілу, достовірно визначити кількість пристроїв, що знаходяться в працездатному стані в довільний момент часу неможливо. Для цього слід використовувати математичний апарат прогнозування числа (4) пристроїв, що знаходяться в працездатному стані, $N(\Delta t)$ в залежності від середньозваженого часу знаходження пристрою в непрацездатному стані і довжини тимчасового інтервалу.

$$N(\Delta t) = N_0 \times (1 - \frac{n(\Delta t) \times \overline{tв}}{\Delta t}, \tag{4}$$

де $N(\Delta t)$ - число пристроїв, що знаходяться в непрацездатному стані на інтервалі часу Δt,

$\overline{tв}$ – середній час знаходження пристрою в непрацездатному стані,

N_0 – число пристроїв, що знаходяться в працездатному стані на момент початку спостереження,

Δt – інтервал часу.

Для оцінки впливу Кг (коефіцієнт готовності) елементів ТКМ на Кг ТКМ в цілому, побудуємо графіки залежності Кг ТКМ для кожної розглянутої топології. З математичної точки зору ТКМ являє собою сукупність двох видів елементів: вузлів зв'язку та ліній зв'язку. Для визначення впливу виду топології на Кг ТКМ, побудуємо графіки залежності Кг ТКМ від Кг кожного з її елементів. При побудові графіків приймемо Кг одного виду елементів стабілізованою, тобто для оцінки впливу Кг вузла мережі на Кг ТКМ приймемо стабілізованою значення Кг ребра мережі, і відповідно для оцінки впливу Кг ребра мережі на Кг ТКМ, приймемо стабілізованою значення Кг вузла мережі. Побудуємо графік залежності Кг формалізованих топологій кожного виду при стабілізованій Кг ребра мережі. Для аналітичного розрахунку і побудови графіка приймемо Кг вузла зв'язку, що змінюються в діапазоні від 0,99 до 0,9999 з кроком 0,00099. Кг ребра мережі (Кгр) приймемо стабілізованою на значенні 0,999. Результати розрахунку зображені на графіку рис. 3.

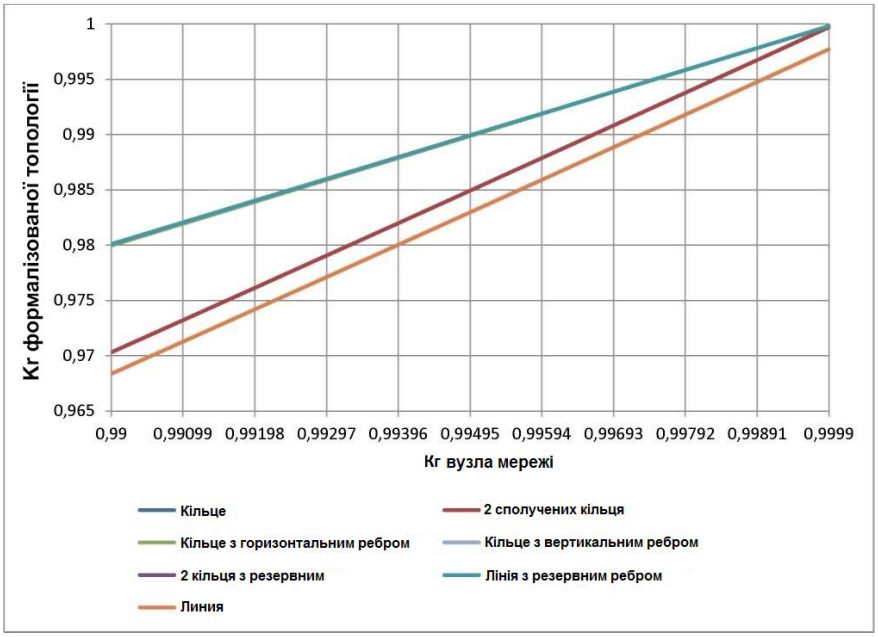

Рис. 3. Графік залежності Кг формалізованих топологій ТКМ від Кг вузла мережі

На графіку рис. 3 наочно доведено, що при низьких значеннях $Кг_у$ при стабілізованому значенні $Кг_р$ Кг лінійної топології з усіма видами резервування практично ідентичні. Топології без повноцінного резервного ребра (лінійна топологія без резервування і з резервуванням тільки ліній зв'язку) не забезпечують достатнього значення Кг сегмента ТКМ.

Проведений аналіз впливу сегментів з резервуванням різної топології на характер убування Кг зі збільшенням довжини ТКМ (числа сегментів). Розрахунки і аналіз отриманих результатів виконані для мережевої топології, зображеної на рис. 3.

Літерами A, B, C, D, E, F, G позначені сегменти топології. Сегменти B, D, A є лінійними топологіями з трьох вузлів, сегменти A, C, E, G є досліджуваний вид топології: кільцеву зображено на рис. 4, кільцеву з зарезервованим вертикальним ребром показано на рис. 5 і кільцеву з зарезервованим горизонтальним ребром зображено на рис. 6.

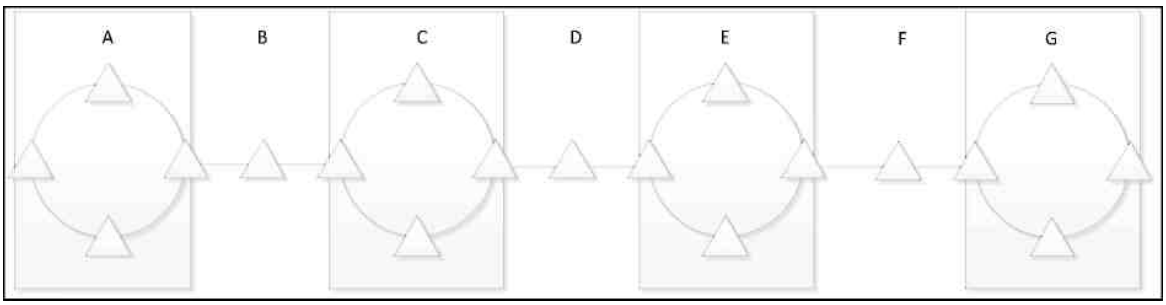

Рис. 4. Неоднорідна топологія з ділянками кільцевої топології без додаткового резервування

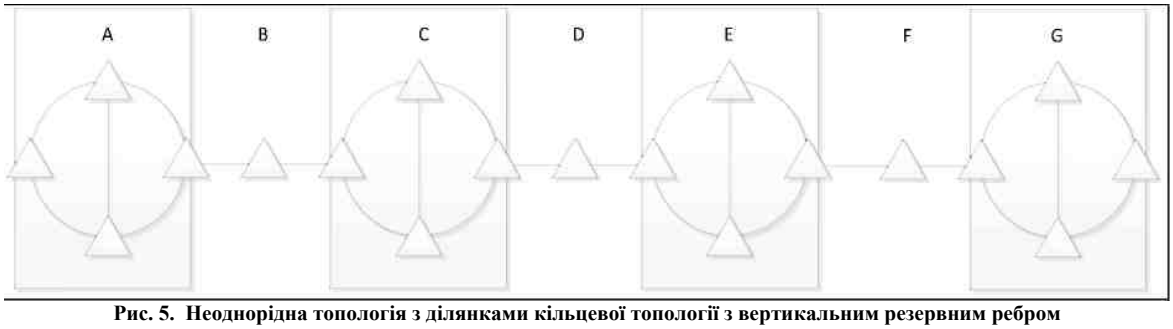

Рис. 5. Неоднорідна топологія з ділянками кільцевої топології з вертикальним резервним ребром

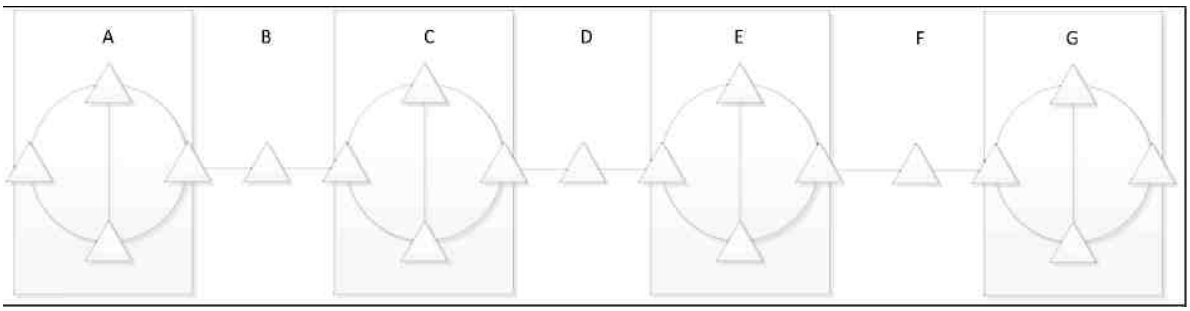

Рис. 6. Неоднорідна топологія з ділянками кільцевої топології з вертикальним резервним ребром

Характер залежності є ламаною лінією, причому найбільший спад Кг відбувається на лінійних ділянках без резервування (B, D, A). Спад Кг на ділянках з зарезервованої топологією набагато менш виражений незалежно від типу резервування. На представленому графіку рис. 7 спостерігається, що Кг топології з кільцевими сегментами помітно нижче, ніж коли зарезервовані сегменти мають кільцеву топологію з резервним ребром. Причому Кг при резервуванні кілець горизонтальними ребрами вище, ніж при резервуванні вертикальними ребрами. Також на рис. 7 науково підтверджується, що чим вище вихідний Кг розглянутого сегмента мережевої топології, тим більше він схильний до зниження при додаванні в ланцюжок додаткових сегментів.

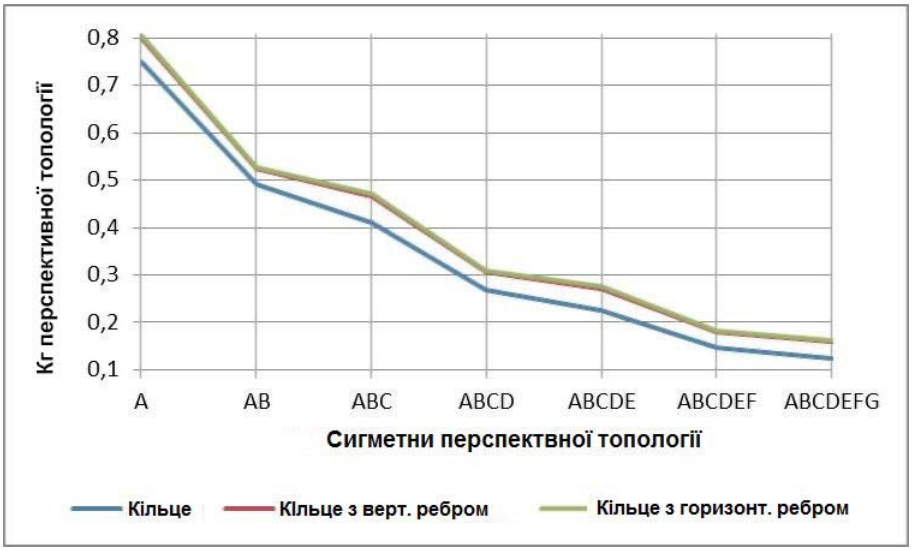

Рис. 7. Вплив типу резервування на Кг неоднорідною топологією при КГЕ л = 0,9

Висновки

В результаті проведеного аналізу можливості застосування математичного і методичного апарату теорії надійності для аналізу структурної надійності складних ТКМ. Як показник ефективності функціонування ТКМ і їх елементів обраний Кг як нормований показник надійності ТКМ і їх елементів. Визначена математична модель, яка описує ймовірність знаходження досліджуваного елемента в працездатному або непрацездатному стані, обумовлених відмовами технічних пристроїв. Виведена розрахункова формула Кг як функції числа відмов і періодів перебування елемента ТКМ в працездатному і непрацездатному стані.

На підставі проведених розрахунків зроблено висновок про можливість впливу на Кг досліджуваних мережевих топологій як за рахунок підвищення Кг складових їх елементів, так і шляхом оптимізації топології за рахунок додавання резервних ребер в різних конфігураціях. Таким чином, обгрунтована можливість підвищення ефективності функціонування ТКМ топологічними методами.

Література

1. Петренко С. Інформаційна безпека: економічні аспекти / С. Петренко, С. Симонов, Р. Кислов // Jet Info, Інформаційний Бюлетень. – 2003. – № 10 (125). – С. 3–24.

2. Методичний документ: Методика визначення загроз безпеки інформації в інформаційних системах [Електронний ресурс]. – Режим доступу : http://fstec.ru/component/attachments/download/812.

3. Шувалов В.П. Забезпечення показників надійності телекомунікаційних систем і мереж / В.П. Шувалов, М.М. Єгунов, Е.А. Мініна Є.М. – Гаряча Лінія – Телеком, 2015. – 168 с.

4. Банк даних загроз безпеки інформації [Електронний ресурс]. – Режим доступу : http://bdu.fstec.ru/documents/files/thrlist.xlsx.

5. Орлов А.І. Експертні оцінки / А.І. Орлов // Журнал «Заводська лабораторія». – 1996. – Т. 62. № 1. – С. 54–60.

6. Агєєв Д.В. Методика опису структури сучасних телекомунікаційних систем з використанням багатошарових графів / Д.В. Агєєв // Східноєвропейський журнал передових технологій. – 2010. – Т. 6 – № 4 (48). – С. 56–59.

7. Касперський К. Техніка мережевих атак / К. Касперський. – М. : СОЛОН-Р, 2001. – 396 с.

8. Романов А.І. Основи теорії телекомунікаційних мереж: навчальний посібник для вузів / О.І. Романов. – К., 2002. – 152 с.

References

1. Petrenko S. Informatsiina bezpeka: ekonomichni aspekty / S. Petrenko, S. Symonov, R. Kyslov // Jet Info, Informatsiinyi Biuleten. – 2003. – Issue 10 (125). – S. 3–24.

2. Metodychnyi dokument: Metodyka vyznachennia zahroz bezpeky informatsii v informatsiinykh systemakh [Elektronnyi resurs]. – Rezhym dostupu : http://fstec.ru/component/attachments/download/812.

3. Shuvalov V.P. Zabezpechennia pokaznykiv nadiinosti telekomunikatsiinykh system i merezh / V.P. Shuvalov, M.M. Yehunov, E.A. Minina Ye.M. – Hariacha Liniia – Telekom, 2015. – 168 s.

4. Bank danykh zahroz bezpeky informatsii [Elektronnyi resurs]. – Rezhym dostupu : http://bdu.fstec.ru/documents/files/thrlist.xlsx.

5. Orlov A.I. Ekspertni otsinky / A.I. Orlov // Zhurnal «Zavodska laboratoriia». – 1996. – T. 62. Issue 1. – S. 54–60.

6. Ahieiev D.V. Metodyka opysu struktury suchasnykh telekomunikatsiinykh system z vykorystanniam bahatosharovykh hrafiv / D.V. Ahieiev // Skhidnoievropeiskyi zhurnal peredovykh tekhnolohii. – 2010. – T. 6 – Issue 4 (48). – S. 56–59.

7. Kasperskyi K. Tekhnika merezhevykh atak / K. Kasperskyi. – M. : SOLON-R, 2001. – 396 s.

8. Romanov A.I. Osnovy teorii telekomunikatsiinykh merezh: navchalnyi posibnyk dlia vuziv / O.I. Romanov. – K., 2002. – 152 s.

Рецензія/Peer review : 13.10.2017 р. Надрукована/Printed :02.12.2017 р.
Рецензент: д.т.н. проф. Сорокатий Р.В.