DOI:**10.33099/2311-7249/2019-35-2-29-34**

УДК: 355.45

***Ярослав В'ячеславович Мельник***
***Віктор Євгенович Бобильов*** *(кандидат військових наук, с.н.с.)*
***Роман Родіонович Тимошенко*** *(кандидат технічних наук)*

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# РЕКОМЕНДАЦІЇ ЩОДО ПОБУДОВИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ОСНОВІ ПОРІВНЯЛЬНОЇ ОЦІНКИ ЇХ СТІЙКОСТІ

*Сучасне інформаційне середовище піддається активному кібернетичному впливу як на окремі комп'ютерні засоби, так і на інформаційно-телекомунікаційні системи та автоматизовані системи органів державного та військового управління, який спрямований на порушення взаємопов'язаних властивостей інформації: конфіденційності, цілісності та доступності. Не зважаючи на впровадження різних методів, спрямованих на підвищення рівня захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах, динаміка збільшення та наслідки кібернетичних загроз, як у світі так і в Україні, залишаються достатньо високими та складають проблему світового рівня. У зв'язку з цим, виникає нагальна потреба забезпечення ефективного функціонування гетерогенних інформаційно – телекомунікаційних мереж (ІТМ) Міністерства оборони та ЗС України в умовах кібератак.*

*Метою даної статті є надання рекомендацій щодо побудови інформаційно-телекомунікаційних мереж на основі порівняльної оцінки стійкості структур інтегрованих комп'ютерних мереж (ІКМ), який дозволяє забезпечити підвищення достовірності результатів порівняльної оцінки структур ІКМ при збільшенні кількості елементів та в умовах впливу на вузли мережі ненавмисних і навмисних перешкод шляхом обліку перспективного зниження значень комплексних показників надійності вузлів ІКМ.*

***Ключові слова:*** *гетерогена мережа, інтегровані комп'ютерні мережі, інформаційно-телекомунікаційні мережі, навмисні та ненавмисні перешкоди, надійність гетеродинних телекомунікаційних мереж.*

## Вступ

**Постановка проблеми.** На даний час у практиці побудови ІКМ використовується усім відомий спосіб порівняльної оцінки структур інформаційно-обчислювальних систем. Головним недоліком вказаного способу є відносно низька достовірність результатів порівняльної оцінки структур інформаційно-обчислювальних систем при збільшенні кількості вузлів зв'язку в ІКМ. Низька достовірність обумовлена:

– великими витратами часу та ресурсів, які необхідні для отримання вихідних даних по великій кількості вузлів ІКМ;

– збільшенням комбінаторної складності рішення задачі пошуку безпечного маршруту при великій кількості вузлів ІКМ;

– зниженням чутливості показника безпеки маршруту, що викликано тим, що при збільшенні кількості вузлів інформаційно-обчислювальних систем буде зростати кількість маршрутів з близьким значенням показника безпеки маршруту.

Інформаційний обмін між абонентами ІКМ здійснюється маршрутизацією пакетів повідомлень через послідовність транзитних вузлів телекомунікаційної мережі загального користування (ТМЗК). Визначення маршруту – складне завдання, особливо коли між абонентами існує безліч альтернативних маршрутів. При цьому вибір маршруту здійснюється оператором зв'язку, який надає послуги передачі інформаційного трафіку між територіально розподіленими сегментами ІКМ через ТМЗК. На кожному вузлі маршруту вибір здійснюється самостійно. В якості критеріїв вибору маршрутів виступають, як технічні характеристики каналу, наприклад:

номінальна пропускна спроможність;

завантаженість каналів зв'язку;

затримки, які вносять канали;

кількість проміжних транзитних вузлів мережі;

надійність каналів та транзитних вузлів мережі;

так і економічні, наприклад вартість передачі трафіку. При цьому економічні показники для комерційних операторів можуть бути більш значимі, ніж технічні.

Для забезпечення передачі інформаційного трафіку між пограничними вузлами ІКМ за допомогою ТМЗК, необхідно здійснювати порівняльну оцінку альтернативних структур ІКМ

на предмет їх стійкості до впливу навмисних та ненавмисних перешкод.

Постановка проблеми. Тому виникає протиріччя між потребою забезпечити достовірність результатів порівняльної оцінки структур ІКМ та збільшенням витрат ресурсів на їх отримання в умовах збільшення кількості вузлів ІКМ та зв'язків між ними, під впливом навмисних та ненавмисних перешкод (ННП). Схильність ІКМ до впливу перешкод вимагає обліку перспективного зниження значень комплексних показників стійкості елементів ІКМ до впливу ННП.

**Аналіз останніх досліджень і публікацій.** Питання дослідження процесів функціонування розподілених інформаційних систем військового призначення висвітлюються у працях А.І. Сбітнєва, В.А. Савченка, О.В. Барабаша, А.В. Зінченка [1, 2] Роботи А.Г. Додонова, М.Г. Кузнєцова досліджують питання живучості інформаційних систем [4]. Дослідження процесів функціонування розподілених баз даних АСУ висвітлені у роботах Т. Коннолли, К. Дейта, Е. Кодда, А.Г. Маміконова та інших [5, 6, 7]. Питанням розробки моделей та алгоритмів управління реплікацією в РБД присвячені роботи Л.І. Мейкшан, Д.Г. Колесникова, О.О. Телятнікова. [8]. Разом з тим, запропоновані в цих роботах моделі та методи оцінювання ефективності функціонування розподілених баз даних АСУ не враховують можливого впливу кібератак. Роботи Ю.І. Субача, В.Л. Бурячка, В.Г. Єсіна присвячені питанням кібербезпеки [3], здебільшого акцентують увагу на методах виявлення та розпізнавання кібервпливів, при цьому процеси функціонування АСУ та вимоги до стійкості в умовах кібератак залишені поза розглядом.

**Метою статті** є визначення шляхів підвищення надійності гетерогенних інформаційно-телекомунікаційних мереж з метою розроблення та впровадження методики побудови гетерогенних інформаційно-телекомунікаційних мереж Міністерства Оборони України та Збройних Сил України із заданим рівнем стійкості до кібератак.

## Виклад основного матеріалу дослідження

Авторами була запропонована методика порівняльної оцінки надійності структур гетерогенних мереж (ГМ), що включають в себе вузли, які не підконтрольні власнику ГМ, та функціонують в умовах впливу ННП, які у свою чергу одержані у результаті вибору альтернативних операторів зв'язку для підключення локальних сегментів ГМ до система зв'язку загального користування (СЗЗК або Інтернет).

Запропонована методика складається з трьох процедур: процедура розкриття структури альтернативних ГМ, одержуваних у результаті вибору того чи іншого оператора зв'язку (провайдера); отримання оцінок надійності альтернативних структур ГМ; порівняльна оцінка отриманих результатів та вибір структури ГМ.

В рамках процедури розкриття структури мережі запропонований порядок дій для вирішення завдання розкриття структури СЗЗК за допомогою стандартних інструментальних засобів ОС і складання єдиного графа ГМ, який має вузли що не підконтрольні власнику ГМ. Процедура отримання оцінок надійності передбачає комп'ютерне моделювання методом, в якому передача інформаційних потоків через ГМ розглядається як просочування однієї речовини через іншу. Знайдені функціональні залежності стійкості структури мережі до впливу ННП порівнюються у процедурі порівняльної оцінки методом інтегральної різниці або на основі експертної оцінки надійності елементів ГМ.

Для цього у методиці, що розроблена, заздалегідь задають параметри ІКМ та формують її топологічну схему. В якості параметрів ІКМ задають ідентифікатори вузлів мережі, наявність зв'язку між ними, параметри надійності вузла (такі, як тип його устаткування, версія встановленого програмного забезпечення, приналежність вузла державній або приватній установі та ін.).

На рис. 1 наведено приклад фрагмента структури ІКМ з вказівкою ідентифікаторів вузлів та абонентів. Обчислюється комплексний показник надійності $П_{комп}$ для кожного вузла ІКМ. Під комплексним показником *i*-го маршруту $П_{комп}$, де $i = 1,2,3, \ldots N$, розуміється нормоване чисельне значення згортки параметрів надійності, яке характеризує стійкість вузлів до впливу ННП. Так як порядок обчислень $П_{комп}$ відомий то розрахунок $П_{комп}$ можна здійснити підсумовуванням, або перемноженням, або середнім арифметичним, або іншою функцією від значення параметрів надійності вузла. Додатково задається мінімально допустиме значення показника надійності $П_{min}$, як мінімальний рівень.

Із сформованої топологічної схеми ІКМ виділяють альтернативні маршрути передачі інформаційного потоку між абонентами, вузли, яких визначаються ідентифікаторами. Для кожної пари альтернативних підключень до ІКМ кореспондуючих абонентів існує кінцева множина альтернативних маршрутів, яка складає структуру ІКМ. Альтернативні маршрути передачі трафіку, які знайдено для кожного *j*-го варіанту зберігають у пам'яті.

Потім порівнюють значення комплексного показника стійкості $П_{комп}$ *i*-го вузла, де $i = 1,2, 3, \ldots,n$, із заздалегідь заданим мінімальним допустимим значенням $П_{min}$. Якщо $П_{копм} < П_{min}$, то вузол запам'ятовується як "ненадійний", інакше – як "надійний".

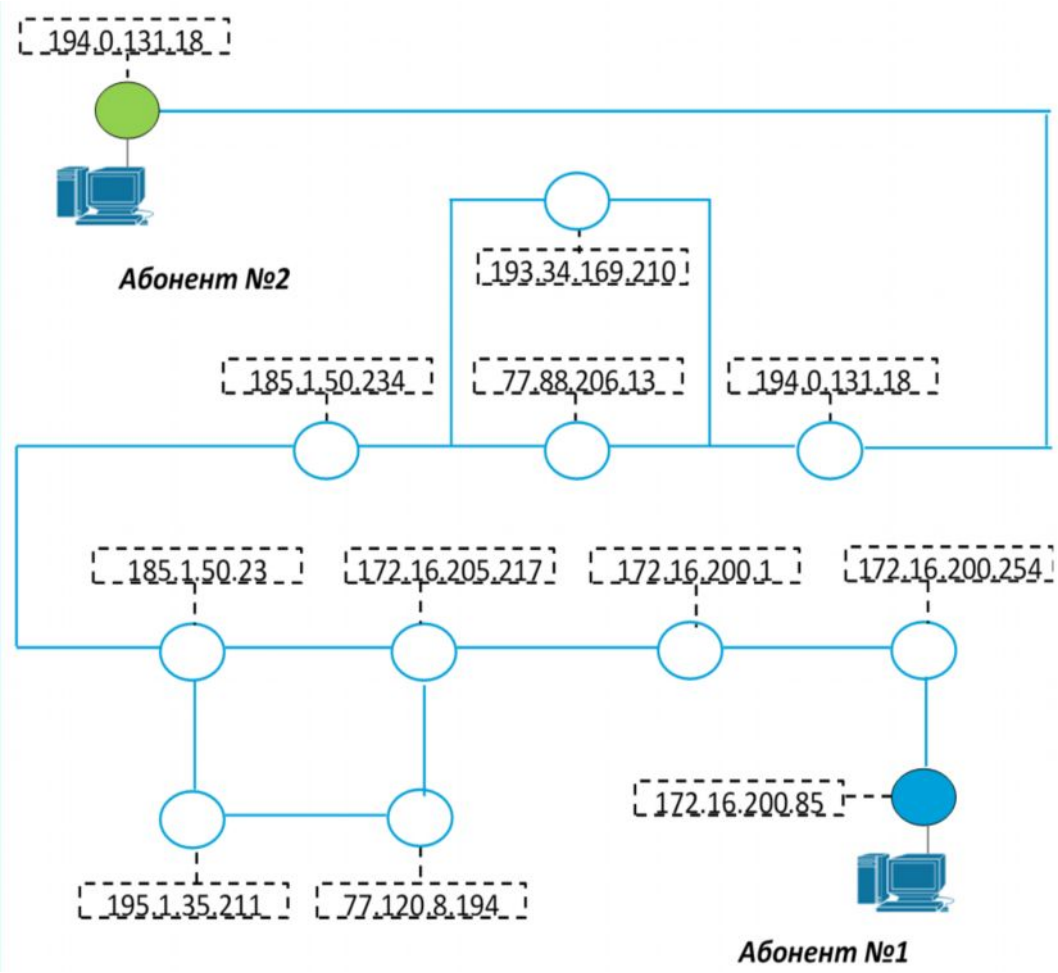


Рис.1. Приклад фрагменту топологічної схеми ІКМ

Запам'ятовується відношення "надійних" вузлів до загальної кількості вузлів мережі як $p^j$.

Розглянемо роботу способу на прикладі ІКМ з регулярною квадратною структурою, у вузлах якої розміщуються вузли, а ребра визначають зв'язки між ними. Нехай $p^j$-я частина вузлів є "надійною" (вузли білого кольору на рис. 2 а), які допускають можливість проходження пакетів між абонентами. "Ненадійні вузли" (вузли чорного кольору) не беруть участь в процесі передачі пакетів повідомлень між абонентами.

З наведеного прикладу, де $p^j = 0,7$, видно, що при наведеній на рис. 2 а і рис. 2, б $p^j$-й частині "надійних" вузлів із загальної їх кількості існує велика кількість альтернативних варіантів маршрутизації пакетів повідомлень між абонентами ІКМ (вузли білого кольору і зв'язки між ними на рис. 2, б), три з яких показані стрілками.

Для того, щоб врахувати перспективне зниження значення комплексного показника стійкості вузла до ННП, необхідно зменшити долю "надійних вузлів" на величину $\Delta p$. Величину $\Delta p$ задають виходячи з необхідної точності результатів розрахунку в інтервалі $\Delta p = 0,0001... 0,1$. На рис. 2, наведена ситуація $p^j = 0,5$. Видно, що існує 4 альтернативних маршрути між абонентами ІКМ, які наведено на рисунку сірими вузлами.

Для обчислення критичного співвідношення "надійних" і "ненадійних" вузлів $p_k^j$. для кожного *j*-го варіанту підключення абонентів, при перевищенні якого вірогідність збереження зв'язку між абонентами різко зростає, необхідно послідовно зменшувати долю "надійних" вузлів на величину $\Delta p$ (де, наприклад, $\Delta p = 0,001$) до того моменту, як кластер "надійних" вузлів, що утворюється, перестане включати абонентів. На рис. 3 наведено приклад структури ІКМ з регулярною решіткою з 1 000 000 елементів (1000 x 1000) і зв'язністю кожного вузла (за виключенням вузлів на границях структури), рівною 4.

Випадкові ітерації, які здійснюються в процесі проведених експериментів за допомогою чисельного моделювання методом статистичних випробувань Монте-Карло, призводять до утворення різних структур з пов'язаних між собою "надійних" вузлів (наведено білим кольором на рис. 3), що мають одну і ту ж закономірність, а саме: критичне співвідношення $p_k^j$ "надійних" і "ненадійних" вузлів для представлених на рис. 2 і 3 структур ІКМ, при якому суміжні "надійні" вузли утворюють кластер, що включає абонентів, уперше виникає при $p^j = p_k^j \approx 0,6$ при зміні $p^j$ від 0 до 1.

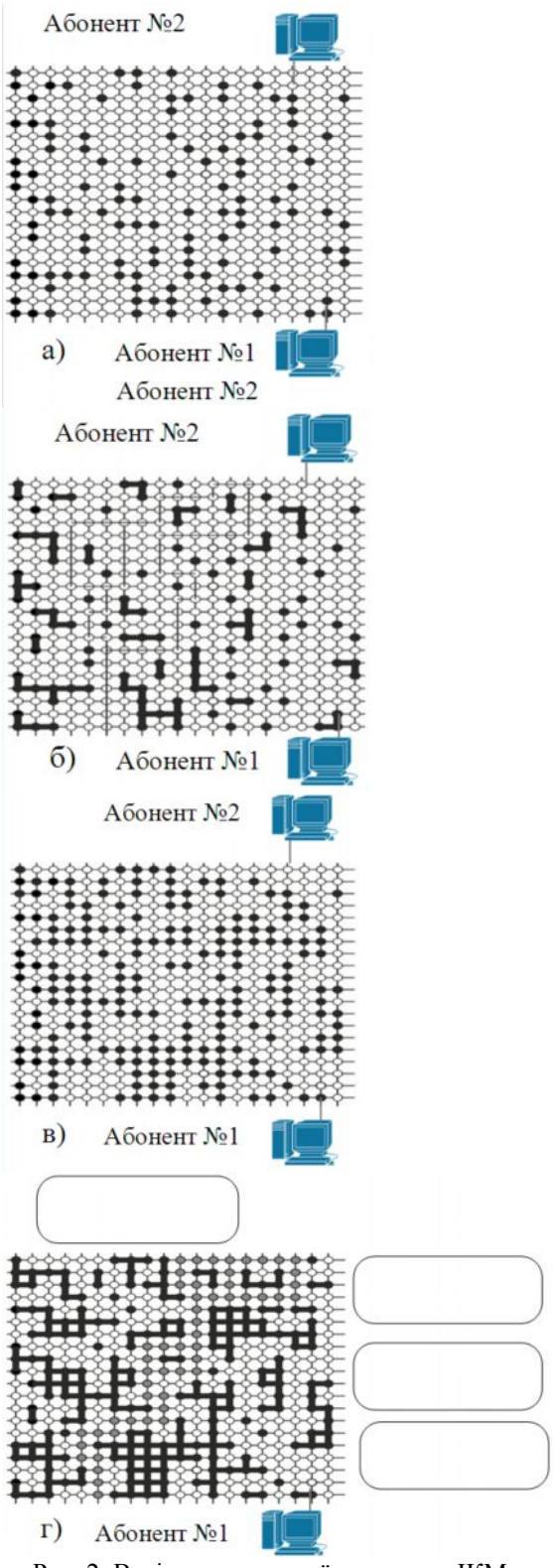


Рис. 2. Варіант регулярної структури ІКМ з різною кількістю “надійних” вузлів

На графіку (рис. 4) наведено результати чисельного моделювання для квадратних решіток різної розмірності. Всього було проведено 7 експериментів, де $L$ = 144, 625, 2 500, 10 000, 40 000, 160 000, 640 000. Для кожної розмірності зроблено по 1000 незалежних випробувань. Наведені результати дозволяють оцінити вірогідність утворення структур, при якій суміжні “надійні” вузли утворюють ланцюжки, що включають абонентів і, таким чином, забезпечують збереження обміну трафіком між ними. Графік ілюструє залежність вірогідності збереження зв’язку $p_{cc}$ між абонентами від долі $p^j$ надійних вузлів в структурі ІКМ.

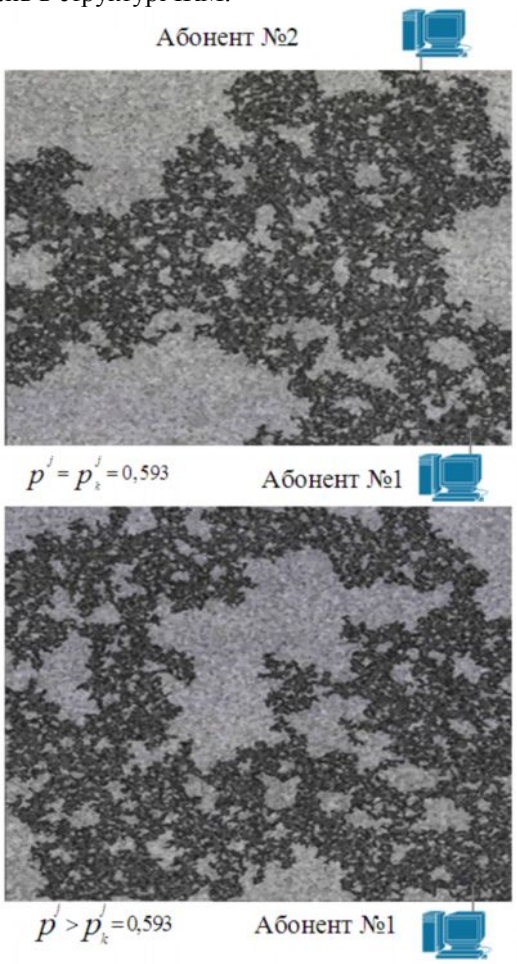


Рис. 3. Приклад структур, які утворюються з пов’язаних між собою "надійних" вузлів на ІКМ з регулярною структурою з 1000000 елементів

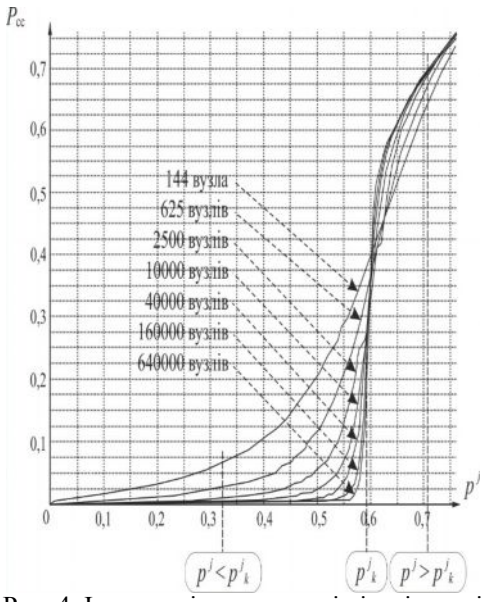


Рис. 4. Ілюстрація залежності вірогідності збереження зв’язку від долі "надійних" вузлів ІКМ в їх загальній кількості

Мала доля "надійних" вузлів ($p^j < p_k^j$) не забезпечує достатню вірогідність збереження зв'язку, тоді як при збільшенні $p^j$ вірогідність збереження зв'язку різко зростає зблизька $p_k^j$ і при $p^j \to 1$ ($p^j > p_k^j$, див. графік на рис. 4) зростає лінійно до значення $p_{cc}$ ($p^j$) = 1.

Наведені дії з обчислення значення $p_k^j$ виконують для кожної альтернативної структури ІКМ. На рис. 5 представлені фрагменти альтернативної регулярної структури ІКМ (решітка Кагоме).

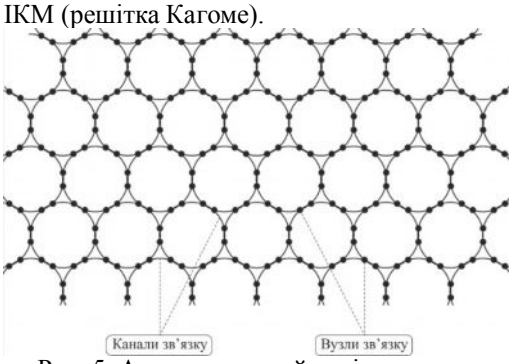


Рис. 5. Альтернативний варіант регулярної структури ІКМ

Результати чисельного моделювання на цій структурі розмірністю $L$ = 625 вузлів (зроблено по 1000 незалежних випробувань) дозволили оцінити вірогідність утворення структур, при якій суміжні "надійні" вузли утворюють кластер, що включає абонентські вузли, що відповідає вірогідності збереження зв'язку $p_{cc}$ між абонентами ІКМ від долі $p^j$ "надійних" елементів в ІКМ.

Графік на рис. 6 ілюструє залежність вірогідності порушення зв'язку $p_{cc}$ між абонентами ІКМ від долі $p^j$ "надійних" елементів в ІКМ.

Після знаходження $p^j$ для кожної альтернативної схеми підключення абонентів ІКМ упорядковують за критерієм зменшення $p_k^j$. Наприклад, для структури, представленої на рис. 5, $p_k^j \approx 0{,}8$.

Це означає, що ця структура менш стійка до дії навмисних і ненавмисних перешкод. Кількість "надійних" вузлів, які потрібні для забезпечення передачі інформації між абонентами, вище, ніж для структури ІКМ представленої на рис. 2. Отже, вибирають перший варіант маршрутизації.

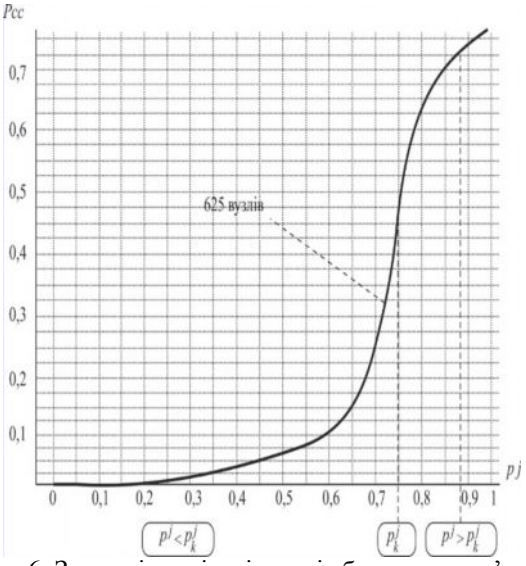


Рис. 6. Залежність вірогідності збереження зв'язку між абонентами ІКМ від долі "надійних" вузлів в їх загальній кількості для альтернативної регулярної структури

## Висновки і перспективи подальших досліджень

Таким чином досягається підвищення достовірності результатів порівняльної оцінки структур ІКМ при збільшенні кількості елементів і в умовах дії навмисних і ненавмисних перешкод шляхом обліку перспективного зниження значень комплексного показника стійкості елементів, що і забезпечує досягнення сформульованого технічного результату. Причому порівняння структур ІКМ здійснюється шляхом оцінки вірогідності утворення структур, при якій суміжні "надійні" вузли утворюють кластери, які включають абонентів, що гарантують доставку повідомлень між ними. Це дозволяє врахувати адаптацію маршрутів передачі пакетів повідомлень між кореспондуючими абонентами до змін структури ІКМ.

## *Література*

**1. Барабаш О.В.** Построение функционально устойчивых распределенных информационных систем / Барабаш О.В. – К.:НАОУ, 2004. – 226 с. **2.** Елементи дослідження складних систем військового призначення: [навч. посіб.] / О.М. Загорка, С.П. Мосов, А.І. Сбітнев, П.І. Стужук. – К.: НАОУ, 2005. – 100 с. **3. Субач І.Ю., Здоренко Ю.М., Фесьоха В.В.** Методика виявлення кібератак типу JS (HTML)/SCRINJECT на основі застосування математичного апарату теорії нечітких множин/ Зб. наук. пр. ВІТІ. – 2018. – Випуск № 4. – С. 125 – 131. **4. Додонов О.Г., Кузнєцова М.Г., Горбачик О.С.** Методи захисту інформації в комп'ютерних системах й мережах: Матеріали круглого столу "Захист інформаційних ресурсів України в інформаційно–телекомунікаційних системах" 23. 05. 2001. — К. : ДСТСЗІ СБ України, 2001. **5. Мамиконова, А.Г.** Автоматизация проектирования АСУ /А.Г. Мамиконова , А.Д. Цвиркун , В.В. Кульба. М., Энергоиздат, 1981.328 с. **6. Дейт, К. Дж.** Введение в системы баз данных / К. Дж. Дейт. М.: Вильяме, 2006. - 1328 с. **7. Коннолли, Томас.** Базы данных. Проектирование, реализация и сопровождение. Теория и практика / Томас Коннолли, Каролин Бегг. -М.: Вильяме, 2003. 1436 с. **8. Мейкшан В.И., Мейкшан Л.И.** Анализ качества функционирования распределенной информационной системы при ограниченной надежности ее элементов // Труды ИВМиМГ СО РАН. – Сер. Информатика. – Вып. 5. – Новосибирск, 2005. – С. 79 – 88.

**РЕКОМЕНДАЦИИ ПО ПОСТРОЕНИЮ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА ОСНОВЕ СРАВНИТЕЛЬНОЙ ОЦЕНКИ ИХ УСТОЙЧИВОСТИ**

***Ярослав Вячеславович Мельник***
***Виктор Евгеньевич Бобвылев (кандидат военных наук, с.н.с.)***
***Роман Родионович Тимошенко (кандидат технических наук)***

***Национальний университет обороны Украины имени Ивана Черняховского, Киев, Україна***

*Современная информационная среда подвергается активному кибернетическому воздействия как на отдельные компьютеры, так и на информационно-телекоммуникационные системы и автоматизированные системы органов государственного и военного управления, которые направленны на нарушение взаимосвязанных свойств информации: конфиденциальности, целостности и доступности. Несмотря на внедрение различных методов, направленных на повышение уровня защищенности информационных ресурсов в информационно-телекоммуникационных системах, динамика увеличения и последствия кибернетических угроз, как в мире так и в Украине, остаются достаточно высокими и составляют проблему мирового уровня. В связи с этим, возникает насущная необходимость обеспечения эффективного функционирования гетерогенных информационно - телекоммуникационных сетей (ИТС) Министерства обороны и Вооруженных Сил Украины в условиях кибератак.*

*Целью данной статьи является выработка рекомендаций по построению информационно-телекоммуникационных сетей на основе сравнительной оценки устойчивости структур интегрированных компьютерных сетей (ИКС), что позволяет обеспечить повышение достоверности результатов сравнительной оценки структур ИКС при увеличении количества ее элементов и в условиях воздействия на узлы сети непреднамеренных и преднамеренных помех путем учета снижения значений комплексных показателей надежности узлов ИКС в перспективе.*

***Ключевые слова:*** *гетерогенная сеть, интегрированные компьютерные сети, информационно-телекоммуникационные сети, умышленные и неумышленные препятствия, надежность гетеродинных телекоммуникационных сетей.*

## RECOMMENDATIONS FOR THE CONSTRUCTION OF INFORMATION AND TELECOMMUNICATION NETWORKS BASED ON THE COMPARATIVE EVALUATION OF THEIR SUSTAINABILITY

***Yaroslav Melnyk***
***Victor Bobylov (Candidate of military sciences, Senior Research Fellow)***
***Roman Timoshenko (Candidate of Technical Sciences )***

***National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine***

*The modern information environment is exposed to active cybernetic influence both on separate computer facilities, as well as on information and telecommunication systems and automated systems of state and military authorities that are aimed at interrupting the interrelated information properties: confidentiality, integrity and accessibility. Despite the introduction of various methods aimed at increasing the security of information resources in the information and telecommunication systems, the dynamics of the increase and the effects of cybernetic threats, both in the world and in Ukraine, remain rather high and constitute a world-class problem. In connection with this, there is an urgent need to ensure the effective functioning of heterogeneous information and telecommunication networks (ITN) of the Ministry of Defense and Armed Forces of Ukraine in the conditions of cyber attacks.*

*The purpose of this article is to provide recommendations on the construction of information and telecommunication networks based on the comparative assessment of the stability of integrated computer networks (CN) structures, which allows to increase the reliability of the results of comparative evaluation of ICN structures with increasing number of elements and under conditions of influence on network nodes of unintentional and intentional obstacles by taking into account the long-term decrease in the values of complex indicators of the reliability of the nodes of the ICN.*

***Key words:*** *heterogyne network, integrated computer networks, information and telecommunication networks, intentional and unintentional obstacles, reliability of heterodyne telecommunication networks.*

## *References*

**1. Barabash O.V.** The construction of functionally stable distributed information systems / Barabash O.V. - K.: NAOU, 2004. - 226 p. **2.** Elements of the study of complex military systems: [curriculum vitae]. manual.] / O.M. Zagorka, SP Mosov, AI Sbitnev, PI Stitug - K .: NAOU, 2005. - 100 p. **3. Subach I.Yu., Zdorenko Yu.M., Fesioha V.V.** The method of detecting a cyberattack type JS (HTML) / SCRINJECT on the basis of the application of a mathematical apparatus of the theory of fuzzy sets / Zb. sciences VITI Ave. - 2018. - Issue number 4. - P. 125 - 131. **4. Dodonov O.G., Kuznetsova M.G., Gorbachik O.S.** Methods of information protection in computer systems and networks: Materials of the round table "Protection of Information Resources of Ukraine in Information and Telecommunication Systems" 23. 05. 2001. - K.: DSTSZI SB of Ukraine, 2001. **5. Mamikonova, A.G.** Automation design ACS / A.G. Mamikonova, A.D. Tsvirkun, V.V. Kulba Moscow, Energoizdat, 1981.328 p. **6. Date, K. Dzh.** Introduction to database systems / K. J. Date. M .: Williams, 2006. - 1328 p. **7. Connolly, Thomas.** Database. Design, implementation and maintenance. Theory and Practice / Thomas Connolly, Caroline Begg. -M .: Williams, 2003. 1436 p. **8. Meikshan V.I., Meikshan L.I.** Analysis of the quality of functioning of a distributed information system with limited reliability of its elements // Proceedings of the ICMMG SB RAS. - Ser. Computer science. - Vol. 5. - Novosibirsk, 2005. - p. 79 - 88..