*УДК 621.391*

Євсєєв С. П.[1], Рзаєв Х. Н.[2], Остапов С. Е.[3], Ніколаєнко В. І.[4]

*[1]Канд. техн. наук, старш. наук. співр., доцент кафедри інформаційних систем, Харківський національний економічний університет ім. С. Кузнеця, Харків, Україна*
*[2]Канд. техн. наук, доцент кафедри «КТ та програмування», Азербайджанський державний Університет Нафти та Промисловості, Баку , Азербайджан*
*[3]Д-р физ.-мат. наук, професор, завідувач кафедрою програмного забезпечення комп'ютерних систем, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна*
*[4]Студентка, Харківський національний економічний університет ім. С. Кузнеця, Харків, Україна*

# ОЦІНКА ОБМІНУ ДАНИМИ В ГЛОБАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ НА ОСНОВІ КОМПЛЕКСНОГО ПОКАЗНИКА ЯКОСТІ ОБСЛУГОВУВАННЯ МЕРЕЖІ

**Актуальність.** Збільшення обсягів даних які циркулюють в комп'ютерних системах і мережах вимагає нових підходів до протоколів і механізмів забезпечення якості обслуговування користувачів і безпеки інформації. Оцінку ефективності обміну даними в комп'ютерній мережі виконують на підставі часткових критеріїв і показників якості обслуговування в протоколах обміну даними в глобальних обчислювальних мережах (ГОМ), що не дозволяє в повній мірі оцінити ефективність якості обслуговування з урахуванням економічних витрат на забезпечення необхідного значення показника якості обслуговування. Актуальним завданням в цьому сенсі є обґрунтування комплексного показника ефективності обміну даними в ГОМ з урахуванням економічних витрат.

**Мета.** Розгляд критеріїв комплексного показника якості обслуговування, ефективності криптографічних засобів захисту інформації, обґрунтування ефективності та обміну даними в ГОМ при різних способах управління обміном на основі комплексного показника ефективності з урахуванням економічних витрат на забезпечення необхідного значення показника якості обслуговування.

**Метод.** Комплексний показник ефективності з урахуванням економічних витрат щодо забезпечення необхідного значення показника якості обслуговування в ГОМ.

**Результати.** Запропоновано методику оцінки ефективності обміну даними в глобальних обчислювальних мережах, яка ґрунтується на простому багатофакторному аналізі. Запропоновано та обґрунтовано комплексний показник ефективності обміну даними, в якому враховано як технічні показники (швидкість передавання даних, ймовірність і час доставки пакету, та інші), так і економічні параметри, наприклад, вартість розгортання та обслуговування мережі тощо.

**Висновки.** Розглянуто методику оцінки ефективності передавання даних в глобальних обчислювальних мережах, яка ґрунтується на простому багатофакторному аналізі. За допомогою запропонованої методики проаналізовано ефективність передавання даних у мережах з різними технологіями, зокрема X.25 (v.34), Frame Relay, Fast Ethernet (0.1Gb, 1Gb, 10Gb, 40 Gb) за єдиними критеріями. Показано, що сьогодні найбільш ефективною технологією за сукупністю параметрів є 10Gb Ethernet. Новизна такого підходу полягає у можливості поєднання технічних та економічних параметрів ефективності обміну даними, що дозволяє ввести комплексний показник ефективності. Практичне використання запропонованого комплексного показника дозволить точніше оцінювати ефективність протоколів обміну даними, які використовуються в глобальних IP-мережах, економічні затрати щодо розгортання та обслуговування мережі, затрат на забезпечення необхідного показника якості обслуговування.

**Ключові слова:** конфіденційність, достовірність, показник якості обслуговування.

## НОМЕНКЛАТУРА

$l_{Д_1}$ – min допустима довжина ключових даних (біт);

$l_{Д_1}$ – max допустима довжина ключових даних (біт);

$n_{пом}$ – кількість помилково прийнятих одиничних елементів;

$n_{заг}$ – загальна кількість переданих одиничних елементів;

$N_{пом}$ – кількість помилково прийнятих кодових послідовностей (пакетів);

$N_{заг}$ – загальна кількість переданих кодових послідовностей (пакетів);

$P_{0пр}$ – ймовірність правильного прийому одиничного елемента;

$P_{пр\ п}$ – ймовірність правильного прийому пакету;

$P_0$ – ймовірність помилкового прийому одиничного елемента, ймовірність помилки біта в каналі передачі даних;

$P_{помп}$ – ймовірність помилкового прийому пакету;

$t_{д'}$ – час доставки пакету з першої посилки;

$\Delta t_д$ – час багатократного повторення передачі інформації при погіршенні якості каналу;

$t_ш$ – час шифрування пакету даних криптоалгоритмом;

$t_{расш}$ – час розшифрування одержувачем пакету даних;

$t_д$ – час доставки пакету;

$\gamma$ – величина, обернена корисній (ефективній) швидкості передачі $R$;

$B$ часова складність (стійкість) використаного в системі шифру – кількість операцій; необхідних для розкриття шифру зловмисником;

$n$ – кількість біт в пакеті;

$h$ – кількість інформаційних розрядів кадру;

$s$ – довжина $S$-кадру;

$C$ – пропускна здатність каналу;

$L$ – довжина лінії зв'язку;

$V_p$ – швидкість поширення сигналу в середовищі;

$t_ш$ – час шифрування I-кадру;

$t_{рш}$ – час розшифрування I-кадру;


DOI 10.15588/1607-3274-2017-1-14

$r$ – кількість виявлених помилок;

$P_0$ – ймовірність помилки в каналі;

$\theta_{ШВ}$ – показник часової складності прямого перетворення (шифрування);

$\theta_{ШЕ}$ – показник ємнісної складності прямого перетворення (шифрування);

$\theta_{РШВ}$ – показник часової складності зворотного перетворення (розшифрування);

$\theta_{РШЕ}$ – показник ємнісної складності зворотного перетворення (розшифрування);

$P$ – ймовірність досягнення мети операції в заданих умовах;

$Q$ – витрати, необхідні для досягнення мети операції;

$W^{(ui)}$ – показник ефективності комп'ютерної мережі при обраній стратегії (методі підвищення достовірності) $u_i$;

$n^{(ui)}$ – кількість інформаційних розрядів пакету при обраній стратегії $u_i$;

$t^{(ui)}$ – час доставки пакету $t$ при вибраній стратегії $u_i$;

$B^{(ui)}$ – кількість операцій, необхідних для розкриття криптоалгоритму зловмисником при обраній стратегії $u_i$;

$\Psi^{(u)}$ – продуктивність обчислювальної системи, доступної криптоаналітику (противнику) при обраній стратегії $u_i$;

$P_{пр\_п}^{(ui)}$ – ймовірність правильної доставки пакету при обраній стратегії;

$U$ – множина допустимих стратегій (методів підвищення достовірності, використовуваних в комп'ютерній мережі);

$W_{eff}$ – показник багатофакторної ефективності, розрахований запропонованим методом;

$Z$ – розмір вікна (для систем с ВЗЗбп «Повернення-на-N»);

$t$ – кратність виправлення помилки (для систем з виправленням помилок);

$P_з$ – задана ймовірність доставки пакету (для систем с ВЗЗпк).

## ВСТУП

Збільшення обсягів даних, що обробляються та передаються в комп'ютерних системах і мережах, перш за все в банківських системах, в системах управління великими фінансовими і нафтовидобувними компаніями, підприємствами енергетичного сектору, транспорту, в системах управління і зв'язку військового призначення вимагає нових підходів до протоколів і механізмів забезпечення безпеки [1–11]. Оцінку ефективності обміну даними в комп'ютерній мережі виконують на підставі часткових критеріїв і показників якості обслуговування в протоколах обміну даними в глобальних обчислювальних мережах [2–4, 12, 13], що не дозволяє в повній мірі оцінити ефективність якості обслуговування з урахуванням економічних витрат на забезпечення необхідного значення показника якості обслуговування.

Актуальним завданням в цьому сенсі є обґрунтування комплексного показника ефективності обміну даними в ГВП з урахуванням економічних витрат.

Метою статті є розгляд критеріїв комплексного показника якості обслуговування, ефективності криптографічних засобів захисту інформації, обґрунтування комплексного показника ефективності обміну даними в глобальних обчислювальних мережах (ГОМ). Для цього проаналізовано показники і критерії безпеки та достовірності передавання даних в

IP-мережах, обґрунтовано ефективність та обмін даними при різних способах управління обміном в протоколах ГОМ на основі комплексного показника ефективності з урахуванням економічних витрат на забезпечення необхідного значення показника якості обслуговування.

## 1 ПОСТАНОВА ЗАДАЧІ

Нехай ми маємо комп'ютерні мережі, що різняться способами управління обміном даних: без зворотного зв'язку з виявленням $r$-кратної помилки; без зворотного зв'язку з виправленням $t$-кратної помилки; з вирішальним зворотним зв'язком і безперервною передачею кадрів (ВЗЗбп) «Повернення-на-N»; з вирішальним зворотним зв'язком і позитивною квитанцією (ВЗЗпк); за параметрами каналу передачі даних: з різною ймовірністю помилки біта, пропускною здатністю каналу передачі даних, довжиною лінії зв'язку, швидкістю поширення сигналу в середовищі тощо; та за загальними параметрами формування комп'ютерної мережі: з різною довжиною інформаційного кадру та іншими параметрами, що залежать від способу управління обміном даних.

Необхідно визначити комплексний показник, що дозволить на основі відомих характеристик кількісно оцінити якість обслуговування мережі. Показник повинен включати показники безпеки та приватні показники системи зв'язку, а також обсяг економічних витрат на програмно-апаратні засоби і технології.

Необхідно також обґрунтувати та дослідити визначений комплексний показник для відомих протоколів глобальних обчислювальних мереж.

## 2 ОГЛЯД ЛІТЕРАТУРИ

На основі загального поняття якості стандарту ICO 8402 були визначені основні терміни в області якості послуг зв'язку (Quality of Service, QoS), вперше наведені в Рекомендації МСЕ-Т Е.800 [14]. В ISO 9000:2005 [15] дано таке визначення QoS: «сукупний показник експлуатаційних характеристик послуги, що визначає ступінь задоволеності користувача послугою». Крім того використовується поняття «якість сприйняття» (Quality Of Experience, QoE), методологія оцінки якого і основне значення параметрів представлені в Рекомендації G.1011 [16]. В цілому якість послуги характеризується сукупністю наступних основних споживчих властивостей [14]: забезпеченістю, зручністю використання, дієвістю, безпекою та іншими властивості, специфічними для кожної послуги.

Крім таких технічних характеристик мереж, як: продуктивність, латентність, масштабованість, ступінь прозорості для кінцевих користувачів, вкрай важливими характеристиками є комплексні показники надійності: коефіцієнт готовності і середній час недоступності в рік. Від показників надійності безпосередньо залежить доступність інформаційних сервісів для користувачів. Крім того, від надійності мережі побічно також залежать продуктивність і латентність мережі, оскільки причиною пожежі і відмов в мережі веде до необхідності повторної передачі блоків даних, а це в підсумку веде до збільшення затримок при передачі і зменшення обсягів, переданих даних в одиницю часу [17].

За останній час у зв'язку з підвищеним інтересом і державною необхідністю розвитку інформаційно-комунікаційного простору країни проводяться дослідження в області побудови ефективних інформаційно-комунікаційних систем (ІКС). Впровадження і якісне використання ІКС вимагає серйозного опрацювання питань не тільки ефективності інформаційного обміну в мережах, але і їх продуктивності в цілому [18].

Під час розгляду ефективності передачі даних в комп'ютерних мережах необхідно враховувати різні параметри систем передачі даних: вартість розгортання мережі, швидкість передавання даних, ймовірність доставки пакету, час доставки пакету, продуктивність мережі тощо. Найчастіше оцінка таких параметрів формується у вигляді формалізованого опису, який не має кількісних характеристик.

Найбільш наближеними до задачі, яка розглядається, є різні методи аналізу захищеності та визначення загального рівня захищеності комп'ютерних мереж, наприклад, що базуються на основі кількісних і якісних методик аналізу ризику, в тому числі на основі математичного апарату теорії ймовірностей, байесовских мереж, теорії можливостей, нечітких множин і т. п. Перспективним напрямком в оцінці рівня захищеності є підходи, засновані на побудові уявлення можливих дій порушників у вигляді дерев або графів атак і наступної перевірки властивостей цього дерева (графа) на основі використання різних методів, наприклад, методів верифікації моделі (model checking), а також обчислення на базі даного подання різноманітних метрик захищеності [19–21].

Також існують методики візуального аналізу мереж, що широко використовуються для аналізу функціонування інформаційної системи. В даний час велика частина існуючих рішень призначена для ефективного контролю периметру мережі. Є різні інструменти для аналізу стану всієї мережі в цілому, моніторингу портів і визначення різних патернів сканування портів, виявлення аномалій в «мережевій поведінці» користувача, в той час як питання візуалізації даних про стан комп'ютерної мережі, підтримки прийняття рішень опрацьовані в меншій мірі та не мають кількісного узагальненого показника.

Для того, щоб розрахувати комплексний показник ефективності комп'ютерних мереж на основі різних технологій, необхідно використовувати багатофакторний аналіз, оскільки в цих випадках враховуються абсолютно різні чинники, кожен з яких може бути розрахований окремо з тих чи інших методик, однак для розрахунку інтегрального показника єдиної кількісної методики не існує.

Отже, найбільш доцільним для оцінки ефективності обслуговування комп'ютерної мережі в якості показника ефективності є використання комплексного показника функціональної ефективності з урахуванням економічних витрат з використанням методів, наведених в [2, 3].

## 3 МАТЕРІАЛИ ТА МЕТОДИ

При розгляді функціонування IP-мережі загальний показник ефективності обміну даними повинен включати в себе показники безпеки і часткові показники системи зв'язку – достовірність і оперативність. Основними критеріями оцінки ефективності секретних систем прийнято вважати наступні [5–9]:

1. Криптографічний стійкість (кількість секретності), яку оцінюють, як складність рішення задачі криптоаналізу найкращим відомим методом.

2. Обсяг ключових даних. Симетрична криптосистема оперує загальними для всіх користувачів секретним ключем. В цьому випадку його поширення вимагає захищених каналів зв'язку, а значить, ключ не повинен бути занадто великим, щоб не виникли проблеми з його розподілом, і не дуже маленьким, щоб його складно було зламати повним перебиранням. У разі асиметричної криптосистеми один з ключів може бути загальнодоступним, його поширюють по відкритих каналах зв'язку.

3. Складність виконання прямого і зворотного криптографічного перетворення (шифрування/розшифрування повідомлень). Ці операції повинні бути по можливості простими, щоб їх легко можна було реалізувати на практиці.

4. Розмноження числа помилок. У деяких типах шифрів помилка в одній літері, допущена при шифруванні або передаванні, призводить до великої кількості помилок в розшифрованому тексті. Природно, бажано мінімізувати це поширення помилок.

5. Збільшення обсягу повідомлення. У деяких типах секретних систем обсяг повідомлення збільшується в результаті операції шифрування. Цей небажаний ефект потрібно мінімізувати.

У табл. 1 наведені розрахункові значення часу, необхідного криптоаналітику при різних довжинах ключа і можливостях доступних обчислювальних потужностей [9].

Аналіз табл. 1 показує, що на сьогоднішній день ключі довжиною <80 біт є нестійкими до зламу методом повного перебирання. З урахуванням прогнозу розвитку обчислювальних засобів на найближчі роки безпечна ефективна довжина ключа сягне значення 100 біт, що відповідає потужності множини ключів $\geq 2^{100}$. Таким чином, загальною вимогою до довжини ключа є умова

$$l_{Д_1} \geq l_K l_{Д_2}.$$

Загальноприйнятими показниками оцінки складності алгоритмів в теорії складності є ємність та часова складність. За визначенням, показником часової складності є час як функція розміру задачі, що розв'язується. Аналогічно, показником ємнісної складності є ємність пам'яті як функція розміру задачі. Введемо відповідні показники складності реалізації криптографічних засобів захисту інформації [10, 11]:

Загальною вимогою до алгоритмів прямого і зворотного перетворення є зменшення перерахованих показників, отже, цільова функція має вигляд:

$$\{\min\theta_{ШВ}, \min\theta_{ШЕ}, \min\theta_{РШВ}, \min\theta_{РШЕ}\}.$$

Таблиця 1 – Розрахункові значення часу, необхідного криптоаналітику для злому ключових даних

| $\psi \setminus l_K$ | 80 біт | 80 біт | 80 біт | 80 біт | 80 біт |
|---|---|---|---|---|---|
| $10^5$ GFlops, (2004–2005р.) | 380 років | $4{\cdot}10^8$ років | $4{,}4{\cdot}10^{20}$ років | $4{,}6{\cdot}10^{26}$ років | $5{\cdot}10^{38}$ років |
| $10^6$ GFlops, (2009–2010р.) | 38 років | $4{\cdot}10^7$ років | $4{,}4{\cdot}10^{19}$ років | $4{,}6{\cdot}10^{25}$ років | $5{\cdot}10^{37}$ років |
| $10^7$ GFlops, (2014–2015р.) | 3,8 років | $4{\cdot}10^6$ років | $4{,}4{\cdot}10^{18}$ років | $4{,}6{\cdot}10^{24}$ років | $5{\cdot}10^{36}$ років |

Під достовірністю розуміють властивість системи, що характеризує її спроможність забезпечувати точне відтворення переданих повідомлень в пунктах прийому [1]. Достовірність залежить від параметрів самої IP-мережі, степеня її технічної досконалості і умов роботи (тип та стан каналів зв'язку, метеорологічні показники, вид та інтенсивність завад, організаційних заходи дотримання правил радіообміну і експлуатації апаратури). Кількісно достовірність передавання може визначатися [1–3]:

– ймовірністю помилкового прийому одиничного елемента (втрат достовірності)

$$P_0 = \lim_{n_{\text{заг}} \to \infty} \frac{n_{\text{пом}}}{n_{\text{заг}}}.$$

– ймовірністю помилкового прийому пакету даних

$$P_{\text{пом п}} = \lim_{N_{\text{озаг}} \to \infty} \frac{N_{\text{пом}}}{N_{\text{заг}}}.$$

– ймовірністю правильного прийому одиничного елемента $P_{0\text{пр}}$ та ймовірністю правильного прийому пакету $P_{\text{пр п}}$, причому

$$P_{0\,\text{пр}} + P_0 = 1;\ P_{\text{пр п}} + P_{\text{пом п}} = 1.$$

Ймовірності помилкового і правильного прийому одиничного елемента ($P_0$ й $P_{0\text{пр}}$) фактично є характеристиками дискретного каналу зв'язку, ймовірності $P_{\text{помп}}$ и $P_{\text{прп}}$ є характеристиками комп'ютерної мережі в цілому, так як вони визначаються не тільки характером та інтенсивністю завад в каналі зв'язку, видом і швидкістю модуляції, а й способом захисту від помилок в системі [1–3].

Час доставки інформації [1–3] – інтервал часу від початку надходження повідомлення даних на вхід передавальної частини комп'ютерної мережі до початку його видачі одержувачу даних приймальною частиною. При передаванні конфіденційної інформації, крім того, в час доставки входить час шифрування відправником пакетів даних і час розшифрування пакетів одержувачем, відповідним криптоалгоритмом.

Аналіз часу шифрування і розшифрування переможців конкурсів криптоалгоритмів AES і NESSIE [8, 9] показує, що для несиметричних алгоритмів складність реалізації криптографічних перетворень на 3–5 порядків вище, ніж у аналогічних систем блоково-симетричних шифрів. Таким чином, в IP-мережі з автоперезапитом (вирішальним зворотним зв'язком) час доставки пакету дорівнює [2–4]:

$t_{\text{д}} = t_{\text{д}}' + \Delta_{\text{д}} + t_{\text{ш}} + t_{\text{расш}}$ – для симетричних криптоалгоритмів,

$t_{\text{д}} = t_{\text{д}}' + \Delta t_{\text{д}} + (t_{\text{ш}} + t_{\text{расш}})^S$ – для асиметричних криптоалгоритмів.

Час $t_{\text{д}}$ доставки повідомлення в задану адресу залежить від багатьох чинників: структури каналів, надійності та завантаження мережі, методу комутації, наявності та характеру завад, що призводять до помилок і повторним передач. Він є випадковою величиною, яка характеризується щільністю розподілу $f(t_{\text{д}})$.

У каналах зв'язку з високою інтенсивністю помилок $P_0$ підвищення достовірності призводить до збільшення часу доставки $t_{\text{д}}$ через зменшення числа повторних посилок пакету, і навпаки, зниження часу доставки $t_{\text{д}}$ за рахунок зменшення кількості повторних посилок пакету веде до зниження достовірності [1]. Однак більшість реальних каналів передачі даних є нестаціонарними, ймовірність одиночної помилки в них змінюється в часі в широких межах від $10^{-9}$ до $10^{-2}$ (див. табл. 8) [1].

Загальною вимогою до достовірності інформації є мінімізація ймовірності помилкового прийому символів повідомлення $P_{\text{пом}}$ або, що еквівалентно, максимізація ймовірності правильного прийому $P_{\text{прп}}$. У той же час на сьогоднішній день вимоги до достовірності інформації істотно зросли і, відповідно до [12, 13], припустима ймовірність помилкового прийому символів повідомлення становить:

$$P_{\text{Д}} < 10^{-7}–10^{-9},$$

в залежності від категорії цінності інформації, її пріоритетності та обладнання. Для того, щоб розрахувати комплексний показник ефективності комп'ютерних мереж передавання даних на основі різних технологій, необхідно використовувати багатофакторний аналіз, оскільки в цих випадках враховуються абсолютно різні чинники: вартість розгортання мережі, швидкість передавання даних, імовірність і час доставки пакету і т. д. Кожен з наведених показників може бути розрахований окремо тим чи іншим методом, однак для розрахунку інтегрального показника єдиної кількісної методики не існує. Зазвичай в таких випадках використовують моделі багатофакторного аналізу, найпростіша з яких була задіяна і в нашому випадку.

Для оцінки комплексного показника ефективності були розроблені опорні таблиці, що дозволяють виділити діапазони зміни необхідних параметрів і визначити їх в умовних балах. Цей простий метод дозволяє, як ми побачимо надалі, отримати досить адекватні результати оцінки, і крім того, об'єднати їх з результатами точних розрахунків по окремих конкретних параметрах. В опорних таблицях 2–7 показані параметри систем передавання даних, які враховуються в інтегральному показнику ефективності.

Таблиця 2 – Вартість розгортання мережі

| Бали | Опис параметру |
|---|---|
| 1 | Дуже висока вартість |
| 2 | Висока вартість |
| 3 | Середня вартість |
| 4 | Низька вартість |
| 5 | Дуже низька вартість |

Таблиця 3 – Швидкість передавання даних

| Бали | Опис параметру |
|---|---|
| 1 | Мала (10Мб/с) |
| 2 | Середня (100 Мб/с) |
| 3 | Висока (1Гб/с) |
| 4 | Дуже висока (10Гб/с) |
| 5 | Надзвичайно висока (40 Гб/с) |

Як бачимо, таким чином вдається описати абсолютно різні параметри, які в інший спосіб аналітично об'єднати практично неможливо.

Для порівняння існуючих технологій передавання даних було відібрано наступні: пакетна комутація за стандартом X.25; Frame Relay; Ethernet, Fast Ethernet; Gigabit, 10 Gb, 40 Gb Ethernet. Порівняльні характеристики зазначених технологій показані в таблицях 8–10.

Використовуючи дані з таблиць 2–10, можна скласти таблицю узагальненої ефективності мереж передачі даних (див. табл. 11), де відібрані показники вже подано в умовних балах.

Таблиця 4 – Ймовірність доставки пакету

| Бали | Опис параметру |
|---|---|
| 1 | Мала (> 0) |
| 2 | Середня (0,95) |
| 3 | Висока (0,97546) |
| 4 | Дуже висока (0,999999) |

Таблиця 5 – Час доставки пакету

| Бали | Опис параметру |
|---|---|
| 1 | Дуже великий (1875 с) |
| 2 | Великий |
| 3 | Середній |
| 4 | Малий (0,006 с) |
| 5 | Дуже малий (0,0003 с) |

Використовуючи дані з таблиць 2–10, можна скласти таблицю узагальненої ефективності мереж передачі даних (див. табл. 11), де відібрані показники вже подано в умовних балах.

Результати, показані в табл. 11, показані на рис. 1, 2.

Для оцінки загальної ефективності функціонування комп'ютерної мережі замість стандартного показника ефективності ми пропонуємо використовувати комплексний показник ефективності з урахуванням економічних витрат, який містить показник багатофакторної ефективності $W_{eff}$.

Структура побудови показника така, що в ньому об'єднані дві основні характеристики системи:

– необхідна ймовірність досягнення мети з необхідним показником забезпечення конфіденційності (інфор-

Таблиця 6 – Затримка пакету

| Бали | Опис параметру |
|---|---|
| 1 | Велика |
| 2 | Середня |
| 3 | Мала |

Таблиця 7 – Продуктивність мережі

| Бали | Опис параметру |
|---|---|
| 1 | Мала |
| 2 | Середня |
| 3 | Висока |

Таблиця 8 – Порівняльна характеристика протоколу Ethernet

| Технологія ГОМ | Вартість | Швидкість передачі даних, Мбіт/с | Довжина пакету, біт | Ймовірність правильної доставки пакету, $P_{пр,п}$ | Час доставки пакету, $t_д$, с |
|---|---|---|---|---|---|
| Ethernet | середня | 10 | 1518 | 0,95 | 0,006 |
| Fast Ethernet | середня | 100 | 1518 | 0,95 | 0,006 |
| Gigabit Ethernet | висока | 1000 | 1518 | 0,99999 | 0,006 |
| 10 GbE | висока | 10 000 | 1518 | 0,99999 | 0,006 |
| 40GbE | висока | 40 000 | 1518 | 0,99999 | 0,006 |

Таблиця 9 – Ймовірнісно-часові характеристики технологій ГОМ

| Технологія ГОМ | Вартість | Швидкість передачі даних, Мбіт/с | Довжина пакету, біт | Ймовірність правильної доставки пакету, $P_{пр.п}$ | Час доставки пакету, $t_д$, с |
|---|---|---|---|---|---|
| X.25 (V.34) | середня | 10 | 1056 | 0,97546 | 1875 |
| Frame Relay | середня | 100 | 12048 | > 0 | 0,0003 |
| Fast Ethernet | середня | 100 | 1518 | 0,95 | 0,006 |

Таблиця 10 – Порівняння Ethernet, пакетної комутації та Frame Relay

| | Fast Ethernet | Пакетна комутація (X.25) | Frame Relay |
|---|---|---|---|
| Мультиплексування з часовим розділенням | Немає | Немає | Немає |
| Статистичне мультиплексування | Так | Так | Так |
| Поділ портів | Так | Так | Так |
| Висока продуктивність | Так | Немає | Так |
| Затримка | Низька | Висока | Низька |

Таблиця 11 – Узагальнена ефективність мереж передачі даних

| Технологія | Вартість | Швидкість | Ймовірність доставки пакету | Час доставки | Затримка пакету | Продуктивність | Узагальнений індекс ефективності | Відносна ефективність,% |
|---|---|---|---|---|---|---|---|---|
| X.25 | 3 | 1 | 3 | 1 | 1 | 1 | 9 | 0,25 |
| Frame Relay | 3 | 2 | 1 | 5 | 3 | 3 | 270 | 7,37 |
| Ethernet | 3 | 1 | 2 | 4 | 3 | 3 | 216 | 5,89 |
| Fast Ethernet | 3 | 2 | 2 | 4 | 3 | 3 | 432 | 11,79 |
| Gigabit Ethernet | 2 | 3 | 4 | 4 | 3 | 3 | 864 | 23,59 |
| 10 Gb Ethernet | 2 | 4 | 4 | 4 | 3 | 3 | 1152 | 31,45 |
| 40 Gb Ethernet | 1 | 5 | 4 | 4 | 3 | 3 | 720 | 19,66 |
| Всього: | | | | | | | 3663 | 100 |

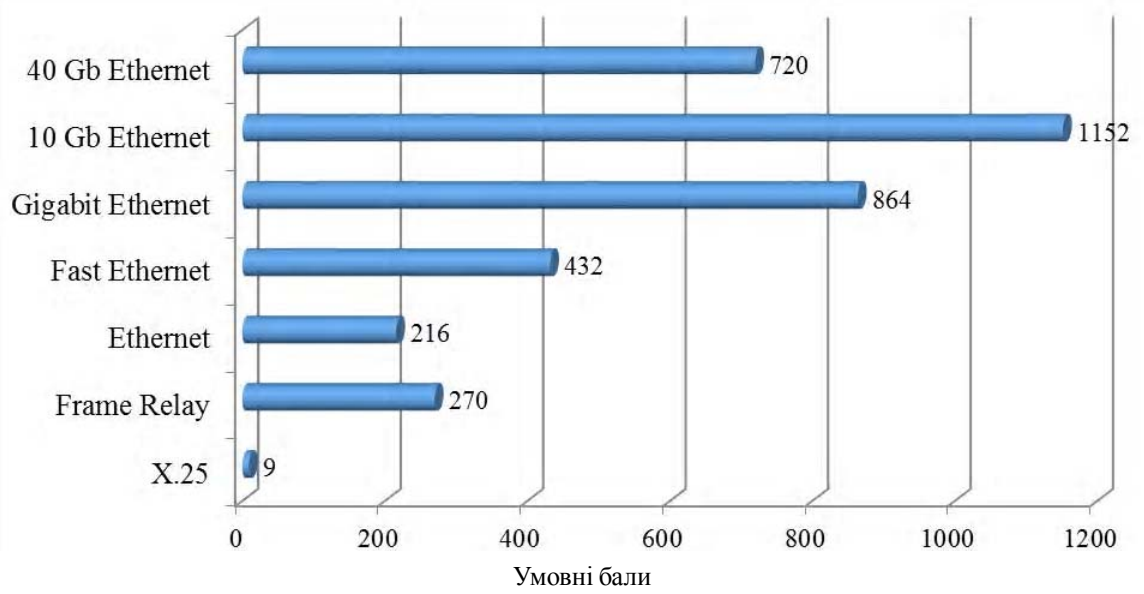


Рисунок 1 – Комплексний показник ефективності різних технологій комп'ютерних мереж

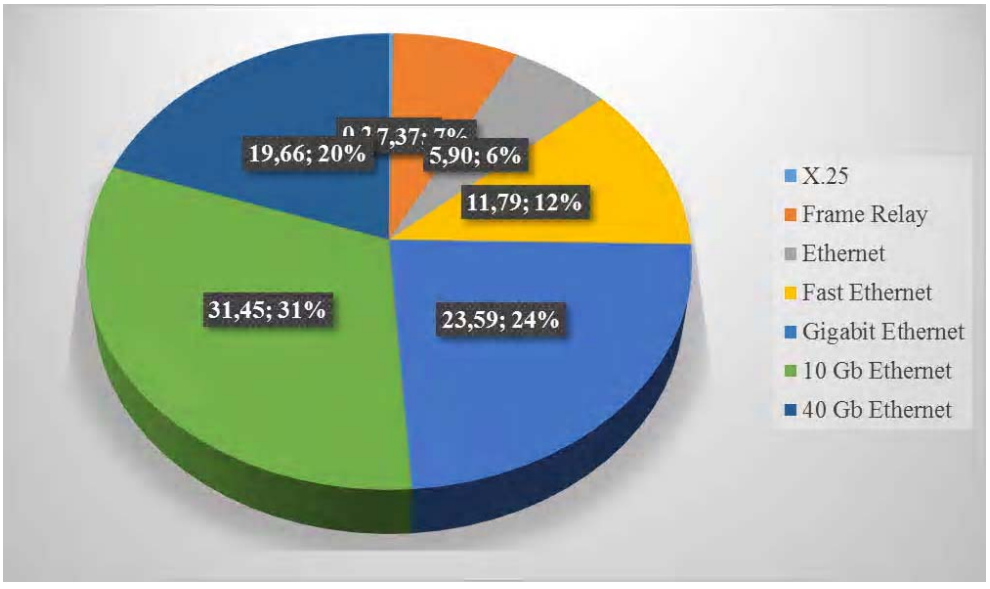


Рисунок 2 – Комплексний показник ефективності різних технологій комп'ютерних мереж

маційної прихованості) в визначених умовах зовнішнього середовища і при певному рівні впливу внутрішніх випадкових факторів;

– витрати, які необхідно здійснити в зазначених умовах для досягнення мети з необхідною ймовірністю і економічні витрати на реалізацію побудови корпоративних мереж з урахуванням необхідного показника якості обслуговування.

Показник функціональної ефективності системи має вигляд

$$W = \frac{P}{Q}.$$

Як ймовірність досягнення мети операції доцільно використовувати ймовірність безпомилкової доставки пакету $P_{\text{прп}}$.

$$P_{\text{пр п}} = (1 - P_0)^n.$$

Витрати, необхідні для забезпечення безпомилкової доставки пакету, визначаються надмірністю. Тому в якості показника вхідної надмірності може виступати коефіцієнт надмірності $\gamma$, яка при фіксованій пропускній спроможності вимірюється кількістю біт інформації, яка міститься в одному пакеті

$$W = \frac{P_{\text{пр п}}}{\gamma}. \quad (1)$$

$$\gamma = \frac{1}{R} = \frac{t_{\text{д}}}{h}. \quad (2)$$

Крім того, для обліку забезпечення необхідної конфіденційності (інформаційної прихованості) переданих даних, до складу показника ефективності необхідно ввести величину, що характеризує часову складність (стійкість) використаного в системі шифру – кількість операцій B, необхідних для розкриття шифру зловмисником. Оскільки дана величина має досить високий порядок (близько $10^{19}$–$10^{77}$), зручніше використовувати її десятковий логарифм. Тоді узагальнений показник ефективності прийме вид

$$W = \frac{h}{t} \cdot \lg B \cdot (1 - P_0)^n.$$

Цей показник містить часткові показники достовірності, конфіденційності та часу доставки даних в комп'ютерній мережі та, по суті, відображає швидкість достовірної та конфіденційної передачі даних комп'ютерною мережею, що дозволяє оцінювати її ефективність в широкому діапазоні інтенсивності помилок в каналі передавання даних при різних швидкостях передавання $R$.

Ймовірність безпомилкової доставки пакету $P_{\text{пр п}}$ за визначенням лежить в діапазоні (0, 1). Ефективна швидкість $R$ і часова складність алгоритму, що реалізує метод криптоаналізу $\lg B$ у загальному випадку лежать в діапазоні (0, +∞). Для переходу з діапазону (0, +∞) в діапазон (0, 1) зручно скористатися формулою

$$x' = \frac{x-1}{x},$$

що має наступні властивості:

$$\lim_{x \to +0} \frac{x-1}{x} = -\infty, \quad \lim_{x \to 1} \frac{x-1}{x} = 0, \quad \lim_{x \to \infty} \frac{x-1}{x} = 1.$$

Замінивши значення $\frac{h}{t}$ и $\lg B$ еквівалентними їм, отримаємо

$$\frac{\frac{h}{t} - 1}{\frac{h}{t}} = \frac{h-t}{h}, \; W = \frac{h-t}{h} \cdot \frac{\lg B - 1}{\lg B} \cdot (1 - P_0)^n.$$

Якщо замість показника часової складності криптоалгоритму $\lg B$ використовувати безпечний час роботи криптоалгоритму

$$T_{\text{Б}_i} = \frac{B_i}{\Psi}.$$

тоді:

$$W = \frac{h-t}{h} \cdot \frac{t-1}{t} \cdot (1 - P_0)^n = \frac{h-t}{h} \cdot \frac{\frac{B}{\Psi} - 1}{\frac{B}{\Psi}} \cdot (1 - P_0)^n =$$

$$= \frac{h-t}{h} \cdot \frac{B - \Psi}{B} \cdot (1 - P_0)^n.$$

Оскільки час доставки пакету $t$, що входить в (2.23), є випадковою величиною, то можливо оцінити тільки його математичне сподівання $m_t$. У цьому випадку вибір оптимальної стратегії функціонування комп'ютерної мережі $u^*$ з множини допустимих стратегій $U$ доцільно здійснювати за критерієм найбільшого середнього результату, тобто

$$W(u^*) = \max_{u_i \in U} W(u_i), \quad (3)$$

$$W(u_i) = \frac{n^{(u_i)} - t^{(u_i)}}{n^{(u_i)}} \frac{B^{(u_i)} - \Psi^{(u_i)}}{B^{(u_i)}} P_{\text{пр п}}^{(u_i)} W_{eff}.$$

При цьому окремі показники повинні задовольняти системі обмежень при мінімізації часу доставки кадру інформації.

$$\{T_{\text{Б}} \geq T_{\text{Д}}, P_{\text{ош}} \leq P_{\text{Д}}, t_{\text{д}} \leq t_{\text{Д}}, W_{eff} \geq W_{\text{Д}}\}, \quad (4)$$

Вибрані комплексний показник і критерій ефективності комп'ютерної мережі дозволяють отримати числові значення, що характеризують швидкість достовірної та конфіденційної передачі даних в ГОМ з урахуванням економічних витрат на їх реалізацію і провести порівняння існуючих протоколів IP-мереж за ефективністю обміну даними між двома вузлами комп'ютерної мережі.

**4 ЕКСПЕРИМЕНТИ**

Для підвищення значення показника функціональної ефективності комп'ютерної мережі використовуються

різні способи управління обміном даними: без зворотного зв'язку з виявленням *r*-кратної помилки; без зворотного зв'язку з виправленням *t*-кратної помилки; з вирішальним зворотним зв'язком і безперервною передачею кадрів (ВЗЗбп) «Повернення-на-N»; з вирішальним зворотним зв'язком і позитивною квитанцією (ВЗЗпк).

Дослідимо комп'ютерні мережі, що використовують дані способи управління обміном даними.

У комп'ютерній мережі, що використовують циклічні коди в режимі виявлення помилок (стратегія $u_1$) значення показника ефективності визначається як [5–8]

$$W(u_1)=\frac{n^{(u_1)}-t^{(u_1)}}{n^{(u_1)}}\frac{B^{(u_1)}-\Psi^{(u_1)}}{B^{(u_1)}}P_{\text{пр п}}{}^{(u_1)}W_{eff}\ , (5)$$

$$t^{(u_1)}=\frac{n}{C}+\frac{L}{V_p}+t_{\text{ш}}+t_{p\text{ш}},$$

$$P_{\text{пр п}}^{(u_1)}=(1-P_0)^n.$$

Для комп'ютерної мережі без зворотного зв'язку при виправленні *t*-кратної помилки циклічним кодом (стратегія $u_2$) значення показника ефективності визначається як:

$$W(u_2)=\frac{n^{(u_2)}-t^{(u_2)}}{n^{(u_2)}}\frac{B^{(u_2)}-\Psi^{(u_2)}}{B^{(u_2)}}P_{\text{пр п}}{}^{(u_2)}W_{eff}, \quad (6)$$

$$t^{(u_2)}=\frac{n}{C}+\frac{L}{V_p}+t_{\text{ш}}+t_{p\text{ш}},$$

$$P_{np\,n}^{(u_2)}=\sum_{i=0}^{t}C_n^iP_0^i(1-P_0)^{n-i}.$$

Для комп'ютерної мережі з вирішальним зворотним зв'язком і безперервним передаванням кадрів «Повернення-на-N» значення показника ефективності визначається як:

$$W(u_3)=\frac{n^{(u_3)}-t^{(u_3)}}{n^{(u_3)}}\frac{B^{(u_3)}-\Psi^{(u_3)}}{B^{(u_3)}}P_{\text{пр п}}{}^{(u_3)}W_{eff}, \quad (7)$$

$$M\left[t^{(u_3)}\right]=\frac{n}{C}+\frac{L}{V_p}+t_{\text{ш}}+t_{p\text{ш}}+$$

$$+\frac{\sum_{i=1}^{r}C_n^i\cdot P_0^i\cdot(1-P_0)^{n-i}+(1-\frac{1}{2^r})\cdot\sum_{i=r+1}^{n}C_n^i\cdot P_0^i\cdot(1-P_0)^{n-i}}{(1-P_0)^n}\times$$

$$\times\left(\frac{n+s}{C}+2\frac{L}{V_p}\right),$$

$$P_{\text{пр п}}^{(u_3)}=\frac{(1-P_0)^n}{1-\sum_{i=1}^{r}C_n^iP_0^i(1-P_0)^{n-i}-(1-\frac{1}{2^r})\cdot\sum_{i=r+1}^{n}C_n^iP_0^i(1-P_0)^{n-i}}\cdot$$

Для комп'ютерної мережі з вирішальним зворотним зв'язком і позитивною квитанцією значення показника ефективності визначається як:

$$W(u_4)=\frac{n^{(u_4)}-t^{(u_4)}}{n^{(u_4)}}\frac{B^{(u_4)}-\Psi^{(u_4)}}{B^{(u_4)}}P_{\text{пр п}}{}^{(u_4)}W_{eff}\ , (8)$$

$$M\left[t^{(u_4)}\right]=\frac{n+s}{C}+2\frac{L}{V_p}+t_{\text{ш}}+t_{\text{рш}}+$$

$$+\frac{\sum_{i=1}^{r}C_n^i\cdot P_0^i\cdot(1-P_0)^{n-i}+(1-\frac{1}{2^r})\cdot\sum_{i=r+1}^{n}C_n^i\cdot P_0^i\cdot(1-P_0)^{n-i}}{(1-P_0)^n}\cdot\frac{n}{C},$$

$$P_{\text{пр п}}^{(u_4)}=(1-P_0)^n\times$$

$$\times\frac{1-\left(\sum_{i=1}^{r}C_n^iP_0^i(1-P_0)^{n-i}+(1-\frac{1}{2^r})\cdot\sum_{i=r+1}^{n}C_n^iP_0^i(1-P_0)^{n-i}\right)^N}{1-\sum_{i=1}^{r}C_n^iP_0^i((1-P_0))^{n-i}-(1-\frac{1}{2^r})\cdot\sum_{i=r+1}^{n}C_n^iP_0^i(1-P_0)^{n-i}}.$$

В результаті розрахунків за допомогою виразів 5–8 отримані числові значення показника ефективності комп'ютерної мережі *W* при зміні ймовірності бітових помилок $P_0$.

Для оцінки показника функціональної ефективності комп'ютерної мережі при різних методах управління обміном даними в КС, в каналах без пам'яті використовуємо такі вирази:

– в комп'ютерної мережі, що використовує циклічні коди в режимі виявлення помилок, значення показника ефективності визначається як [9–12]

$$W(u_1)=\frac{n^{((u_1)}-t^{((u_1)}}{n^{(u_1)}}\frac{B^{((u_1)}-\Psi^{(u_1)}}{B^{(u_1)}}P_{np\,n}{}^{(u_1)}W_{eff}\ , (9)$$

– для комп'ютерної мережі без зворотного зв'язку при виправленні *t*-кратної помилки циклічним кодом, значення показника ефективності визначається як [9–12]

$$W(u_2)=\frac{n^{(u_2)}-t^{(u_2)}}{n^{(u_2)}}\frac{B^{(u_2)}-\Psi^{(u_2)}}{B^{(u_2)}}P_{np\,n}{}^{(u_2)}W_{eff}\ , (10)$$

– для комп'ютерної мережі з вирішальним зворотним зв'язком і безперервним передаванням кадрів «Повернення-на-*N*» значення показника ефективності визначається як [9–12]

$$W(u_3)=\frac{n^{(u_3)}-t^{(u_3)}}{n^{(u_3)}}\frac{B^{(u_3)}-\Psi^{(u_3)}}{B^{(u_3)}}P_{\text{пр п}}{}^{(u_3)}W_{eff}\ , (11)$$

– для комп'ютерної мережі з вирішальним зворотним зв'язком і позитивною квитанцією кадрів значення показника ефективності визначається як [9–12]

$$W(u_4) = \frac{n^{(u_4)} - t^{(u_4)}}{n^{(u_4)}} \frac{B^{(u_4)} - \Psi^{(u_4)}}{B^{(u_4)}} P_{\text{пр п}}{}^{(u_4)} W_{eff}^{(u_4)}. \quad (12)$$

## 5 РЕЗУЛЬТАТИ

На рис. 3 наведені результати дослідження відповідних стратегій в каналах передачі без пам'яті за допомогою виразів 9–12.

Аналіз результатів, наведених на рис. 3 показує на необхідність використання протоколів керування обміном даними з автоперезапитом (вирішальним зворотним зв'язком і позитивною квитанцією, з ВЗЗ і безперервним передаванням кадрів «Повернення-на-N»), як у широкосмугових цифрових каналах (виділених цифрових лініях, оптоволоконних кабелях), так і в повітряних лініях з $P_0 = 10^{-3}$–$10^{-2}$.

Детальне дослідження статистичних властивостей послідовностей помилок в реальних каналах зв'язку [1] показало, що помилки залежні та мають тенденцією до скупчення (пакетування), тобто між ними існує певна залежність – кореляція. Велику частину часу інформація проходить каналами зв'язку без спотворень, а в окремі моменти часу виникають згущення помилок, так звані пакети (пачки, групи) помилок, всередині яких ймовірність помилки виявляється значно вищою за середню ймовірність помилок для значного часу передачі. В таких умовах способи захисту, оптимальні для гіпотези незалежних помилок, виявляються неефективними при використанні їх в реальних каналах зв'язку. Для обліку статистичних властивостей послідовностей помилок в реальних каналах зв'язку розглянемо модель каналу з пам'яттю.

У даній моделі у вихідні дані замість ймовірності помилки біта $P_0$ необхідно задати наступні чотири канальних параметри:

– ймовірність виникнення пакету помилок $P_{\text{пом}}$;

– ймовірність помилки усередині пакету дорівнює $P_{\varepsilon}$;

– математичне сподівання $m_{ln}$ довжини пакету помилок;

– середньоквадратичне відхилення $\sigma_{ln}$ довжини пакету помилок.

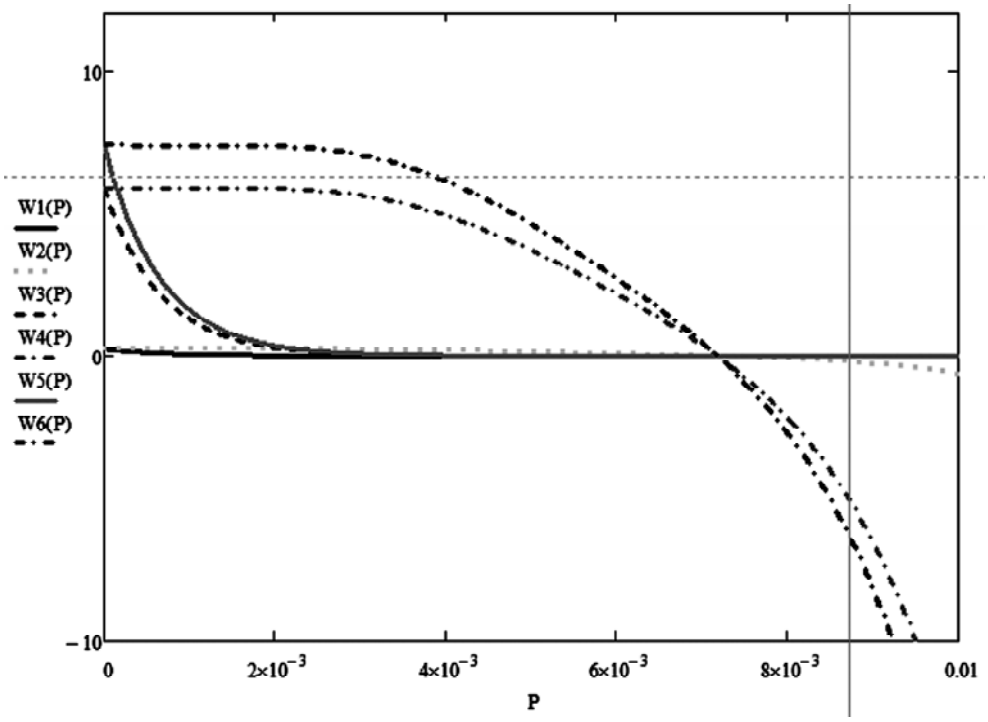


Рисунок 3 – Показник функціональної ефективності в каналах без пам'яті

Позначення:

1 – Повернення-на-N (протокол із симетричною криптосистемою) для X25;

2 – Састрі (з вирішальним зворотним зв'язком) (протокол із симетричною криптосистемою) для X25;

3 – Повернення-на-N для Ethernet;

4 – Састрі для Ethernet;

5 – Повернення-на-N для Frame Relay;

6 – Састрі для Frame Relay.

Примітка:

$C$ = 56000 біт/с; $C1 = 10^6$ біт/с; $C2 = 10^9$ біт/с; $L$ = 1000 км; $V_p = 3 \cdot 10^8$ м/с; $r$ = 16; $t$ = 8; $n$ = 1024 й $n_{\text{разр. метод}}$ = 512 біт; $k$ = 16; $P_{\text{зад}}$ = 0,95; $t_{\text{ш\_сим}} = t_{\text{рш\_сим}}$ = 0,01 с;

$t_{\text{ш\_асим}} = t_{\text{рш\_асим}} = 10^2$ с; $t_{\text{ш\_разр. метод}} = t_{\text{рш\_разр. метод}} = 10^{-2}$ с; $B = 10^{24}$ и $B_{\text{разр. метод}} = 10^{30}$; $\psi = 10^{15}$; EconEth = 5,7; EconFR = 7,37; EconX = 0,25

При розрахунках приймалось: $P_{\text{пом}} = 10^{-5}$, $10^{-2}$; $P_{\varepsilon} = 0{,}8$ ; $m_{l_n} = 10$; $\sigma_{l_n} = 2$.

Для каналів з пам'яттю в комп'ютерної мережі, що використовують циклічні коди в режимі виявлення помилок, значення показника ефективності визначається як

$$W(u_1) = \frac{n^{(u_1)} - t^{(u_1)}}{n^{(u_1)}} \frac{B^{((u_1))} - \Psi^{(u_1)}}{B^{(u_1)}} P_{\text{пр п}}{}^{(u_1)} W_{eff}, \quad (13)$$

$$t^{(u_1)} = \frac{n}{C} + \frac{L}{V_p} + t_{\text{ш}} + t_{\text{рш}},$$

$$P_{\text{пр п}}^{(u_1)} = 1 - \sum_{i=0}^{\infty} \left\{ \left[ 1 - (1 - P_n)^{n+i} \right] \left[ \Phi\left( \frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left( \frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}.$$

Для комп'ютерної мережі без зворотного зв'язку при виправленні $t$-кратної помилки циклічним кодом значення показника ефективності визначається як

$$W(u_2) = \frac{n^{(u_2)} - t^{(u_2)}}{n^{(u_2)}} \frac{B^{(u_2)} - \Psi^{(u_2)}}{B^{(u_2)}} P_{\text{пр п}}{}^{(u_2)} W_{eff}, \quad (14)$$

$$m_t^{(u_2)} = \frac{n}{C} + \frac{L}{V_p} + t_{\text{ш}} + t_{\text{рш}},$$

$$P_{\text{пр п}}^{(u_2)} = 1 - \sum_{i=0}^{\infty} \left\{ \left[ 1 - (1 - P_{\text{п}})^{n-t+i} \right] \left[ \Phi\left( \frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left( \frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}.$$

Для комп'ютерної мережі з вирішальним зворотним зв'язком і безперервною передачею кадрів «Повернення-на-N» значення показника ефективності визначається як

$$W(u_3) = \frac{n^{(u_3)} - t^{(u_3)}}{n^{(u_3)}} \frac{B^{(u_3)} - \Psi^{(u_3)}}{B^{(u_3)}} P_{\text{пр п}}{}^{(u_3)} W_{eff}, \quad (15)$$

$$m_t^{(u_3)} = \frac{n}{C} + \frac{L}{V_p} + t_{\text{ш}} + t_{\text{рш}} +$$

$$+ \frac{\sum_{i=0}^{\infty} \left\{ \left[ 1 - (1 - P_n)^{n+i} \right] \cdot \left[ \Phi\left( \frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left( \frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\} \left\{ 1 - \frac{1}{2^r} \left[ \frac{1}{2} - \Phi\left( \frac{r+1-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}}{1 - \sum_{i=0}^{\infty} \left\{ \left[ 1 - (1 - P_n)^{n+i} \right] \left[ \Phi\left( \frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left( \frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}} \times \left( \frac{n+s}{C} + 2\frac{L}{V_p} \right),$$

$$P_{\text{пр п}}^{(u_3)} = \frac{1 - \sum_{i=0}^{\infty} \left\{ \left[ 1 - (1 - P_n)^{n+i} \right] \left[ \Phi\left( \frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left( \frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}}{1 - \sum_{i=0}^{\infty} \left\{ \left[ 1 - (1 - P_n)^{n+i} \right] \left[ \Phi\left( \frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left( \frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\} \left\{ 1 - \frac{1}{2^r} \left[ \frac{1}{2} - \Phi\left( \frac{r+1-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}}.$$

Для комп'ютерної мережі з вирішальним зворотним зв'язком і позитивною квитанцією кадрів значення показника ефективності визначається як

$$W(u_4) = \frac{n^{(u_4)} - t^{(u_4)}}{n^{(u_4)}} \frac{B^{(u_4)} - \Psi^{(u_4)}}{B^{(u_4)}} P_{\text{пр п}}{}^{(u_4)} W_{eff}, \quad (16)$$

$$t^{(u_4)} = \frac{n+s}{C} + 2\frac{L}{V_p} + t_{\text{ш}} + t_{\text{рш}} + \frac{n}{C} \times$$

$$\times \frac{\sum_{i=0}^{\infty} \left\{ \left[ 1 - (1 - P_n)^{n+i} \right] \cdot \left[ \Phi\left( \frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left( \frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\} \left\{ 1 - \frac{1}{2^r} \left[ \frac{1}{2} - \Phi\left( \frac{r+1-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}}{1 - \sum_{i=0}^{\infty} \left\{ \left[ 1 - (1 - P_n)^{n+i} \right] \left[ \Phi\left( \frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left( \frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}},$$

$$P_{\text{пр п}}^{(u_4)} = 1 - \sum_{i=0}^{\infty} \left\{ \left[ 1 - (1 - P_n)^{n+i} \right] \left[ \Phi\left( \frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left( \frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\},$$

$$\frac{1 - \sum_{i=0}^{\infty} \left\{ \left[ 1 - (1 - P_n)^{n+i} \right] \cdot \left[ \Phi\left( \frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left( \frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\} \left\{ 1 - \frac{1}{2^r} \left[ \frac{1}{2} - \Phi\left( \frac{r+1-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}^N}{1 - \sum_{i=0}^{\infty} \left\{ \left[ 1 - (1 - P_n)^{n+i} \right] \left[ \Phi\left( \frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left( \frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\} \left\{ 1 - \frac{1}{2^r} \left[ \frac{1}{2} - \Phi\left( \frac{r+1-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}}.$$

В результаті розрахунків за допомогою виразів 13–16 отримано числові значення показника ефективності комп'ютерної мережі $W$ при зміні ймовірності виникнення пакету помилок $P_n$.

На рис. 4 наведені результати дослідження відповідних стратегій в дискретних каналах передачі з пам'яттю за допомогою виразів 13–16.

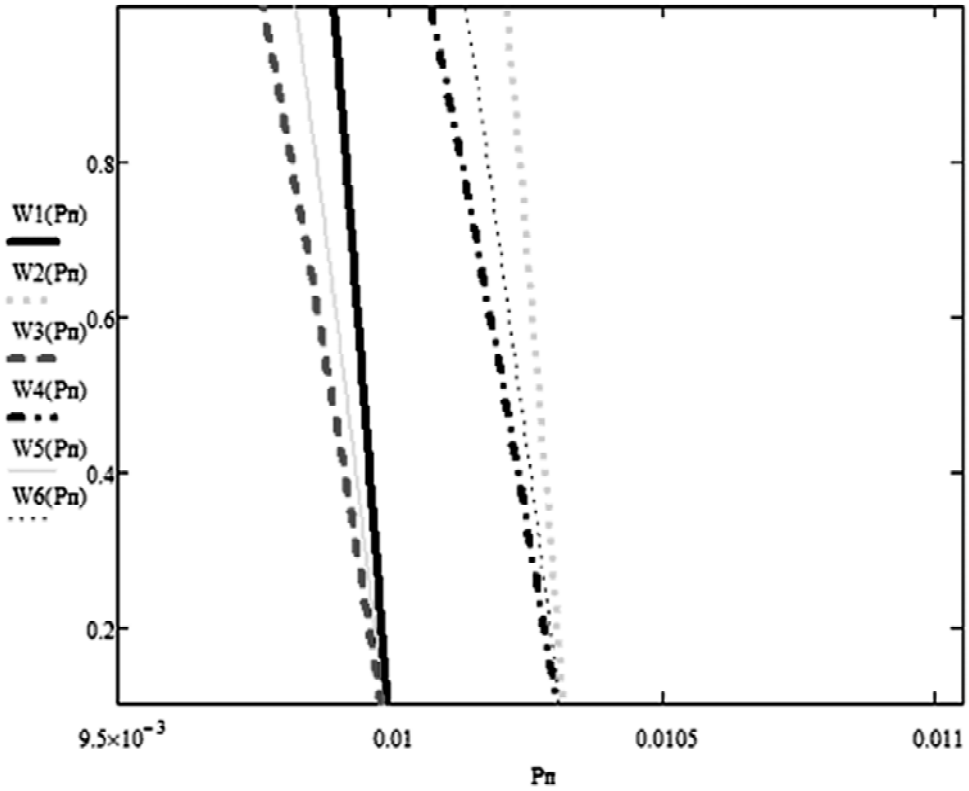


Рисунок 4 – Показник функціональної ефективності в каналах с пам'яттю

Позначення:

1 – Повернення-на-N (протокол із симетричною криптосистемою) для X25;

2 – Састрі (з вирішальним зворотним зв'язком) (протокол із симетричною криптосистемою) для X25;

3 – Повернення-на-N для Ethernet;

4 – Састрі для Ethernet;

5 – Повернення-на-N для Frame Relay;

6 – Састрі для Frame Relay.

Примітка:

$C$ = 56000 біт/с; $C1 = 10^6$ біт/с; $C2 = 10^9$ біт/с; $L$ = 1000 км; $V_p = 3 \cdot 10^8$ м/с; $r$ = 16; $t$ = 8; $n$ = 1024 і $n_{\text{разр. метод}}$ = 512 біт; $k$ = 16; $P_{\text{зад}}$ = 0,95; $t_{\text{ш\_сим}} = t_{\text{рш\_сим}} = 10^{-2}$ с;

$t_{\text{ш\_асим}} = t_{\text{рш\_асим}} = 10^2$ с; $t_{\text{ш\_разр. метод}} = t_{\text{рш\_разр. метод}} = 10^{-2}$ с; B = $10^{24}$ и $B_{\text{разр.метод}} = 10^{30}$; $\psi = 10^{15}$; EconEth = 5,7; EconFR = 7,37; EconX = 0,25.

## 6 ОБГОВОРЕННЯ

Запропонована нами методика врахування економічної ефективності дозволяє отримати досить адекватний результат (див. табл. 11 та рис. 1–2). З них видно, що сьогодні найбільш ефективним за сукупністю наведених показників є 10Gb Ethernet. Звичайний, популярний, добре налагоджений для сьогоднішніх комунікацій Fast Ethernet зі швидкістю передачі даних 100 Мб вже не в повній мірі справляється зі зростаючим трафіком. Зі збільшенням останнього все більшої популярності набуватиме Gigabit Ethernet для повсякденних потреб. Це тим більш стає зрозумілим, якщо врахувати, що основний контент, що передається сьогодні по каналах зв'язку, – це мультимедіа. Останнім часом вимоги споживачів до якості зображення і звуку стрімко зростають, розглядаються нові стандарти HD-відео та інтернет-телебачення, які вимагають все більших бітрейтів. Тому зростання швидкостей передавання даних і якості каналів зв'язку є об'єктивною необхідністю.

Однак поки 40Gb Ethernet залишається досить дорогим для кінцевого споживача, що не дозволяє класифікувати його як оптимальну мережеву інфраструктуру.

Разом з тим, 10Mb Ethernet, Frame Relay, не кажучи вже про пакетної комутації X.25, розглядаються навіть таким простим аналізом, як застарілі технології, що не відповідають поточним реаліям.

Показник багатофакторної ефективності $W_{eff}$ в подальшому використано для розгляду моделей каналів передавання даних.

Аналіз отриманих результатів (див. рис. 3–4) свідчить, що при розгляді моделі каналу з пам'яттю показники ефективності обміну даними в КМ різко падають, за рахунок пакетування помилок в реальних каналах зв'язку. Протоколи з автоперезапитом задовольняють вимогам узагальненого показника ефективності тільки при використанні розробленої криптосистеми в протоколах з вирішальним зворотним зв'язком і безперервним передаванням кадрів «Повернення-на-N» або з вирішальним

зворотним зв'язком і позитивною квитанцією, яка дозволяє інтегровано забезпечити потрібні параметри надійності й безпеки системи. Разом з тим, аналіз рис. 3–4 демонструє, що застосування криптосистем знижує вимоги з оперативності – час формування пакету даних зростає на 20%.

## ВИСНОВКИ

З наведеного вище можна зробити такі висновки:

1. В роботі розглянуто методику оцінки ефективності передавання даних в глобальних телекомунікаційних мережах, яка ґрунтується на простому багатофакторному аналізі.

2. Новизна такого підходу полягає у можливості поєднання технічних та економічних параметрів ефективності обміну даними, що дозволяє ввести комплексний показник ефективності.

3. За допомогою запропонованої методики проаналізовано ефективність передавання даних у мережах з різними технологіями, зокрема X.25 (v.34), Frame Relay, Fast Ethernet (0.1Gb, 1Gb, 10Gb, 40 Gb) за єдиними критеріями.

4. Показано, що сьогодні найбільш ефективною технологією за сукупністю параметрів є 10Gb Ethernet.

5. Практичне використання запропонованого показника дозволить точніше оцінювати ефективність протоколів обміну даними, які використовуються в глобальних IP-мережах.

Перспективним напрямком подальших досліджень є розроблення інтегрованого показника якості на основі методики, яка наведена в роботі, з урахуванням економічної складової витрат на протидію або зменшення впливу загроз на основні активи комп'ютерних мереж та практична оцінка якості обслуговування на основі корпоративної мережі підприємства.

## ПОДЯКИ

Дослідження проведені в рамках Держбюджетної прикладній науково-дослідній роботи №40/2015-2016 «Планування, моніторинг, самооцінка діяльності і розвитку вищого навчального закладу». Державний реєстраційний номер 0115U002377, кафедри інформаційних систем ХНЕУ ім. С. Кузнеця, «Розробка програмно-апаратної системи для дослідження параметрів нано- та мікроб'єктів у колоїдних розчинах та твердих тілах» (номер державної реєстрації 0115U003240) за підтримки Міністерства освіти і науки України.

## СПИСОК ЛІТЕРАТУРИ

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр. / Пер. с англ. – М. : Издательский дом «Вильямс», 2003. – 1104 с.
2. Сумцов Д. В. Общий показатель эффективности передачи данных в компьютерной сети / Д. В. Сумцов, Б. П. Томашевский, А. М. Носик // Системи обробки інформації. – 2009. – №7(79). – С. 85–90.
3. Эффективность обмена данными в компьютерной сети при различных способах управления обменом / [С. П. Евсеев, Д. В. Сумцов, О. Г. Король, Б. П. Томашевский] // Збірник наукових праць. Донецький інститут залізничного транспорту. – 2009. – Випуск 17. – С. 33–45.
4. Анализ эффективности передачи данных в компьютерных системах с использованием интегрированных механизмов обеспечения надежности и безопасности / [С. П. Евсеев, Д. В. Сумцов, О. Г. Король, Б. П. Томашевский] // Восточно-европейский журнал передовых технологий. – 2010. – № 2/2(44). – С. 45–49.
5. Ленков С. В. Методы и средства защиты информации: [в 2 т.] / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко ; (под ред. В. А. Хорошко). – К. : Арий, 2008. – Т.1. Несанкционированное получение информации. – 464 с.
6. Ленков С. В. Методы и средства защиты информации: [в 2 т.] / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко ; (под ред. В. А. Хорошко). – К. : Арий, 2008. – Т. 2. Информационная безопасность. – 344 с.
7. Молдовян Н.А. Криптография: от примитивов к синтезу алгоритмов / Н. А. Молдовян, А. А. Молдовян, М. А. Еремеев. – СПб. : БХВ – Петербург, 2004. – 448 с.
8. Остапов С. Э. Технологии защиты информации / С. Э. Остапов, С. П. Евсеев, О. Г. Король. – Черновцы : Издательский дом «РОДОВИД», 2014. – 428 с.
9. Столлингс В. Криптография и защита сетей: принципы и практика / В. Столлингс ; [Пер. с англ.]. – 2-е изд. – М. : ИД «Вильямс», 2001. – 672 с.
10. Концепция создания системы контроля качества предоставления услуг связи в Российской Федерации [Электронный ресурс] : – Режим доступа : http://minsvyaz.ru/ru/documents/4668.
11. ISO 9000:2005. Системы менеджмента качества. Основные положения и словарь [Электронный ресурс] : – Режим доступа : https://www.iso.org/obp/ui#iso:std:iso:9000:ed-3:v1:ru.
12. Стандарт ГОСТ РВ 51987 «Информационная технология, комплекс стандартов на АС. Требования и показатели качества функционирования информационных систем» [Электронный ресурс]. – Режим доступа : http://gearletitbit.weebly.com/blog/gost-rv-51987-2002.
13. Бойко А. А. Система показателей качества баз данных автоматизированных систем / А. А. Бойко, С. А. Гриценко, В. Ю. Храмов // Вестник ВГУ, серия: Системный анализ и информационные технологии. – 2010. – № 1. – С. 39–45.
14. Оценка сложности алгоритмов [Электронный ресурс] : – Режим доступа : http://habrahabr.ru/post/104219/
15. Вялый М. Н. «Сложность вычислительных задач» : [Электронный ресурс]. – Режим доступа: http://www.nature.ru/db/msg.html?mid
16. МСЭ-Т G.1011 Справочное руководство по существующим стандартам методик определения оценки пользователем качества услуги (QoE). [Электронный ресурс]. – Режим доступа : http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11931&lang=ru
17. Каяшев А. И. Анализ показателей надежности локальных компьютерных сетей / А. И. Каяшев, П. А. Рахман, М. И. Шарипов // Вестник УГАТУ, Уфа. –2013, Т. 17, № 5 (58). – С. 140–149.
18. Степаненко Е. В. Использование метрологических принципов для оценки эффективности работы инфокоммуникационных систем и сетей // Психолого-педагогический журнал Гаудеамус. – 2010. – № 2 (16). – С. 1–4.
19. Пятибратов А. П. Вычислительные системы, сети и телекоммуникации : учебное пособие / А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко ; под ред. А. П. Пятибратова. – М. : КНОРУС, 2013. – 376 с.
20. Бройдо В. Л. Вычислительные системы, сети и телекоммуникации : учебник для вузов 4-е изд. / В. Л. Бройдо, О. П. Ильина. – СПб. : Питер, 2011. – 560 с.
21. Модели и методы управления сетевыми ресурсами в информационно-телекоммуникационных системах : монография / [С. Г. Семенов, А. А. Смирнов, Е. В. Мелешко]. – Харьков : НТУ «ХПИ», 2011. – 212 с.

Стаття надійшла до редакції 22.09.2016.
Після доробки 09.12.2016.

Евсеев С. П.[1], Рзаев Х. Н.[2], Остапов С. Е.[3], Николаенко В. И.[4]

[1]Канд. техн. наук, старш. научн. сотр., доцент кафедры информационных систем, Харьковский национальный экономический университет им. С. Кузнеца, Харьков, Украина

[2]Канд. техн. наук, доцент кафедры «КТ и программирование», Азербайджанский государственный Университет Нефти и Промышленности, Баку, Азербайджан

[3]Д-р физ.-мат. наук, профессор, заведующий кафедрой программного обеспечения компьютерных систем, Черновицкий национальный университет имени Юрия Федьковича, Черновцы, Украина

[4]Студентка, Харьковский национальный экономический университет им. С. Кузнеца, Харьков, Украина

**ОЦЕНКА ОБМЕНА ДАННЫМИ В ГЛОБАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ НА ОСНОВЕ КОМПЛЕКСНЫХ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ОБСЛУЖИВАНИЯ СЕТИ**

**Актуальность.** Увеличение объемов данных, циркулирующих в компьютерных системах и сетях требует новых подходов к протоколам и механизмам обеспечения качества обслуживания пользователей и безопасности информации. Оценку эффективности обмена данными в компьютерной сети выполняют на основании частных критериев и показателей качества обслуживания в протоколах обмена данными в глобальных вычислительных сетях (ГВС), что не позволяет в полной мере оценить эффективность качества обслуживания с учетом экономических затрат на обеспечение требуемого значения показателя качества обслуживания. Актуальной задачей в этом смысле является обоснование комплексного показателя эффективности обмена данными в ГВС с учетом экономических затрат.

**Цель.** Рассмотрение критериев комплексного показателя качества обслуживания, эффективности криптографических средств защиты информации, обоснование эффективности и обмена данными в ГВС при различных способах управления обменом на основе комплексного показателя эффективности с учетом экономических затрат на обеспечение требуемого значения показателя качества обслуживания.

**Метод.** Комплексный показатель эффективности с учетом экономических затрат по обеспечению необходимого значения показателя качества обслуживания в ГВС.

**Результаты.** Предложена методика оценки эффективности обмена данными в глобальных вычислительных сетях, основанная на простом многофакторном анализе. Предложен и обоснован комплексный показатель эффективности обмена данными, в котором учтены, как технические характеристики (скорость передачи данных, вероятность и время доставки пакета, и т.д.), так и экономические параметры, например, стоимость развертывания и обслуживания сети и тому подобное.

**Выводы (научная новизна и практическая значимость).** Рассмотрена методика оценки эффективности передачи данных в глобальных вычислительных сетях, основанная на простом многофакторном анализе. С помощью предложенной методики проанализирована эффективность передачи данных в сетях с различными технологиями, в частности X.25 (v.34), Frame Relay, Fast Ethernet (0.1Gb, 1Gb, 10Gb, 40 Gb) по единым критериям. Показано, что сегодня наиболее эффективной технологией по совокупности параметров является 10Gb Ethernet. Новизна такого подхода заключается в возможности сочетания технических и экономических параметров эффективности обмена данными, позволяет ввести комплексный показатель эффективности. Практическое использование предложенного комплексного показателя позволит точнее оценивать эффективность протоколов обмена данными, которые используются в глобальных IP-сетях, экономические затраты по развертыванию и обслуживанию сети, затраты на обеспечение необходимого показателя качества обслуживания.

**Ключевые слова:** конфиденциальность, достоверность, показатель качества обслуживания.

Yevseiev S. P.[1], Rzayev H. N.[2], Ostapov S. E.[3], Nikolaenko V. I.[4]

[1]Ph.D., Associate Professor of Information Systems Departments Kharkiv National Economic University. S. Kuznets, Kharkiv, Ukraine

[2]Ph.D., Associate Professor of «CT and programming», Departments Azerbaijan State University of Oil and Industry, Baku, Azerbaijan

[3]Head of the Software Department, Yu. Fed'kovych Chernivtsi National University, Chernivtsi, Ukraine

[4]Student of S. Kuznets Kharkiv National Economic University. S. Kuznets, Kharkiv, Ukraine

**DATA EXCHANGE EVALUATION IN GLOBAL NETWORKS BASED ON INTEGRATED QUALITY INDICATOR OF SERVICE NETWORK**

**Context**. Increasing amount of data circulating in computer systems and networks requires new approaches to the protocols and mechanisms to ensure the user experience and security of information.

Evaluation of the communication effectiveness in a computer network is performed on the basis of particular criteria and quality of service indicators in the data exchange protocols in a wide area network (WAN), which does not allow to fully appreciate the quality of service efficiency, taking into account the economic costs of providing the required values of service indicators quality. An important task in this sense is the study of the complex index of efficiency of data exchange in the global computer networks, taking into account the economic costs.

**Objective**. Consideration of the criteria of the complex index service quality, efficiency of cryptographic information protection, and effectiveness of communication in global computer networks in various ways on the basis of the exchange control integrated efficiency indicator, taking into account the economic costs of providing the required quality of service parameter value.

**Method**. The complex index of efficiency, taking into account the economic costs to ensure the required quality of service parameter values in a global computer networks.

**Results**. It was offered the methodics of evaluating data effectiveness in global computer networks, based on a simple multifactor analysis. Proposed and justified a comprehensive indicator of the effectiveness of data exchange, which takes into account, as the specifications (baud rate, probability and packet delivery time, etc.), and economic parameters, such as cost of deployment and network maintenance, and so on.

**Conclusions.** The method of evaluating the effectiveness of the data on a global computer networks, based on a simple multivariate analysis is offered.

With the proposed method analyzed the data transmission efficiency in networks with different technologies, such as X.25 (v.34), Frame Relay, Fast Ethernet (0.1Gb, 1Gb, 10Gb, 40 Gb) on the same criteriaIt is shown that today the most effective technology on the set of parameters a 10Gb Ethernet. The novelty of this approach lies in the possibility of technical and economic parameters combination of the communication effectiveness, it allows to introduce an integrated performance indicator. The practical use of the proposed complex index will more accurately assess the effectiveness of communication protocols, which are used in global IP-based networks, the economic costs of deployment and maintenance of the network, the cost of providing the required quality of service indicator.

**Keywords**: privacy, reliability, quality service indicator.

## REFERENCES


1. Skljar B. Cifrovaja svjaz'. Teoreticheskie osnovy i prakticheskoe primenenie. Izd. 2-e, ispr./ Per. s angl. Moscow, Izdatel'skij dom «Vil'jams», 2003, 1104 p.
2. Sumcov D. V., Tomashevskij B. P., Nosik A. M. Obshhij pokazatel' jeffektivnosti peredachi dannyh v komp'juternoj seti, *Sistemi obrobki informacii,* 2009, No. 7(79), pp. 85–90.
3. Evseev S. P., Sumcov D. V., Korol' O. G., Tomashevskij B. P. Jeffektivnost' obmena dannymi v komp'juternoj seti pri razlichnyh sposobah upravlenija obmenom, *Zbirnik naukovih prac'. Donec'kij institut zaliznichnogo transportu*, 2009, Vipusk 17, pp. 33–45.
4. Evseev S. P., Sumcov D.V., Korol' O. G., Tomashevskij B. P. Analiz jeffektivnosti peredachi dannyh v komp'juternyh sistemah s ispol'zovaniem integrirovannyh mehanizmov obespechenija nadezhnosti i bezopasnosti, Vostochno-evropejskij zhurnal peredovyh tehnologij, 2010, № 2/2(44), pp. 45–49.
5. Lenkov S. V., Peregudov D. A., Horoshko V. A.; (pod red. Horoshko V. A.) Metody i sredstva zashhity informacii: [v 2 t.]. Kiev, Arij, 2008, Vol. 1, Nesankcionirovannoe poluchenie informacii, 464 p.
6. Lenkov S. V., Peregudov D. A., Horoshko V. A. (pod red. V. A. Horoshko). Metody i sredstva zashhity informacii: [v 2 t.]. Kiev, Arij, 2008, Vol. 2, Informacionnaja bezopasnost', 344 p.
7. Moldovjan N. A., Moldovjan A. A., Eremeev M. A. Kriptografija: ot primitivov k sintezu algoritmov. Sankt-Peterburg, BHV-Peterburg, 2004, 448 p.
8. Ostapov S. Je., Evseev S. P., Korol' O. G. Tehnologii zashhity informacii. Chernovcy, Izdatel'skij dom «RODOVID», 2014, 428 p.
9. Stollings V. Per. s angl. 2-e izd. Kriptografija i zashhita setej: principy i praktika. Moscow, ID «Vil'jams», 2001, 672 p.
10. Koncepcija sozdanija sistemy kontrolja kachestva predostavlenija uslug svjazi v Rossijskoj Federacii [Jelektronnyj resurs]. Rezhim dostupa: http://minsvyaz.ru/ru/documents/4668/
11. ISO 9000:2005. Sistemy menedzhmenta kachestva. Osnovnye polozhenija i slovar' [Jelektronnyj resurs]. Rezhim dostupa: https://www.iso.org/obp/ui#iso:std:iso:9000:ed-3:v1:ru
12. Standart GOST RV 51987 «Informacionnaja tehnologija, kompleks standartov na AS. Trebovanija i pokazateli kachestva funkcionirovanija informacionnyh sistem» [Jelektronnyj resurs] : – Rezhim dostupa : http://gearletitbit.weebly.com/blog/gost-rv-51987-2002.
13. Bojko A. A., Gricenko S. A., Hramov V. Ju. Sistema pokazatelej kachestva baz dannyh avtomatizirovannyh sistem, *Vestnik VGU, serija: Sistemnyj analiz i informacionnye tehnologii,* 2010, No. 1, pp. 39–45.
14. Ocenka slozhnosti algoritmov [Jelektronnyj resurs]. Rezhim dostupa : http://habrahabr.ru/post/104219/
15. Vjalyj M. N. «Slozhnost' vychislitel'nyh zadach»: [Jelektronnyj resurs]. Rezhim dostupa: http://www.nature.ru/db/msg.html?mid
16. MSJe-T G.1011 Spravochnoe rukovodstvo po sushhestvujushhim standartam metodik opredelenija ocenki pol'zovatelem kachestva uslugi (QoE). [Jelektronnyj resurs]. Rezhim dostupa: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11931&lang=ru
17. Kajashev A. I., Rahman P. A., Sharipov M. I. Analiz pokazatelej nadezhnosti lokal'nyh komp'juternyh setej, Vestnik UGATU, Ufa, 2013, Vol. 17, No. 5 (58), pp. 140–149.
18. Stepanenko E. V. Ispol'zovanie metrologicheskih principov dlja ocenki jeffektivnosti raboty infokommunikacionnyh sistem i setej, Psihologo-pedagogicheskij zhurnal Gaudeamus, 2010, No. 2 (16), pp. 1–4.
19. Pjatibratov A. P., Pjatibratov A. P., Gudyno L. P., Kirichenko A. A.; pod red. Pjatibratova A. P. Vychislitel'nye sistemy, seti i telekommunikacii : uchebnoe posobie. Moscow, KNORUS, 2013, 376 p.
20. Brojdo V. L., Il'ina O. P. Vychislitel'nye sistemy, seti i telekommunikacii: Uchebnik dlja vuzov.4-e izd. Sankt-Peterburg, Piter, 2011, 560 p.
21. Semenov S. G., Smirnov A. A., Meleshko E. V. Modeli i metody upravlenija setevymi resursami v informacionno-telekommunikacionnyh sistemah: monografija. Har'kov, NTU «HPI», 2011, 212 p.