УДК 621.391

О.Г. Король

Харківський національний економічний університет імені Семена Кузнеця, Харків

ОЦІНКА ЯКОСТІ ОБСЛУГОВУВАННЯ ГЛОБАЛЬНОЇ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЙ ETHERNET ЗА ДОПОМОГОЮ КОМПЛЕКСНОГО ПОКАЗНИКА

У статті проведена оцінка якості обслуговування користувачів глобальної обчислювальної мережі Ethernet на основі комплексного показника, що об'єднує технічні та економічні показники. На основі аналізу методик оцінки економічного збитку (методики оцінки ризиків)для проведення інтегрованої оцінки якості обслуговування пропонується використовувати методику Fair, що дозволяє отримати як якісний, так і кількісний показник збитку.

Ключові слова: *комплексний інтегрований показник якості обслуговування, методика оцінки збитку (ризику), глобальні мережі Ethernet.*

Вступ

Сучасні технології глобальних й локальних обчислювальних мереж (ЛОМ, ГОМ) поширюють галузі їх використання, й разом з зростанням обчислювальних можливостей дозволяють підвищити якість обслуговування своїх клієнтів. Проведений аналіз сучасних протоколів ГОМ показав, що основними вимогами до якості обслуговування є надійність та безпека інформації яка циркулює в протоколах відкритих систем, основною технологією останнього десятиліття, яка використовується на канальному рівні в ГОМ є технологія *Ethernet*. 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 [3; 5; 6; 9; 10; 11; 13; 16; 17; 18; 20; 21], що не дозволяє в повній мірі оцінити ефективність якості обслуговування з урахуванням економічних витрат на забезпечення необхідного значення показника якості обслуговування. В роботах авторів [3; 5; 6; 15; 19; 20; 21] пропонується комплексний показник якості обслуговування, який дозволяє інтегровано оцінити якість обслуговування за показниками надійності (вірогідності), безпеки (конфіденційності) оперативності та економічної складової на основі глобальних протоколів *X.25, Frame Relay, Fast Ethernet* та різних стратегій (протоколів *ARQ*) обміну даними. Актуальним завданням в цьому сенсі є обгрунтування комплексного показника ефективності обміну даними в ГОМ з урахуванням економічних витрат на основі оцінки перспективних технологій *Ethernet 10Gb, 40 Gb*.

Метою статті є оцінка якості обслуговування користувачів глобальної обчислювальної мережі *Ethernet 10Gb, 40 Gb*.на основі комплексного показника, що об'єднує технічні та економічні показники. На основі аналізу методик оцінки економічного збитку для проведення інтегрованої оцінки якості обслуговування пропонується використовувати методику Fair, що дозволяє отримати як якісний, так і кількісний показник збитку.

1. Аналіз сучасних методик оцінки ризиків

Аналіз ситуації в країні і в світі показує, що без управління ризиками вже неможливо забезпечити стабільність і уникнути глобальних криз [1; 2; 4; 7; 8; 12; 14].

Оцінка рівня ризиків інформаційної безпеки в ЛОМ й ГОМ є найбільш складним і відповідальним моментом, оскільки саме від її результатів залежать подальші дії організації. Проведений аналіз показав, що методи оцінки ризиків підрозділяються на дві категорії – якісні та кількісні.

Кількісні методи використовують вимірні, об'єктивні дані для визначення вартості активів, імовірність втрати і пов'язаних з ними ризиків. Мета полягає в тому, щоб обчислити числові значення для кожного з компонентів, зібраних в ході оцінки ризиків та аналізу витрат і переваг.

Якісні методи використовують відносний показник ризику або вартості активу на основі рейтингу або поділ на категорії, такі як низький, середній, високий, не важливо, важливо, дуже важливо, чи за шкалою від 1 до 10. Якісна модель оцінює дії й імовірності виявлених ризиків швидким і економічно ефективним способом. Набори ризиків записані і проаналізовані в якісній оцінці ризику, та можуть послужити основою для цілеспрямованої кількісної оцінки.

Раніше кількісні підходи використовувалися частіше. Однак, останнім часом використання суворо кількісних управлінь ризиками. Зазвичай призводить до важкої, тривалої роботи, і немає великих переваг перед якісним методом оцінки ризиків. Комбінація кількісного і якісного методу являє собою змішану сукупність переваг і недоліків вище згаданих методів (табл. 1).

Таблиця 1

Переваги та недоліки методів оцінки ризиків

+/–	Кількісний	Якісний
Переваги	- ризики є пріоритетними фінансових наслідків; - активи є пріоритетними фінансових цінностей; - отримання спрощених результатів управління ризиком та поверненням інвестицій у забезпечення безпеки; - результати можуть бути виражені в управлінській специфічній термінології (наприклад, грошові значення і ймовірність виражається у вигляді певного відсотка); - точність має тенденцію до збільшення з плином часу, так як організація постійно веде записи даних.	- Забезпечує прозорість і розуміння класифікації ризику; - можливість досягти консенсусу; - немає необхідності визначати фінансову вартість активів; - легше залучити людей, які не є експертами в області комп'ютерної безпеки.
Недоліки	- Вплив значення, привласнених ризикам на підставі суб'єктивних думок учасників; - процес для досягнення надійних результатів і консенсусу займає багато часу; - розрахунок може бути складним і трудомістким; - результати представлені тільки в грошовому еквіваленті і їх складно інтерпретувати для "нетехнічних людей"; - процес вимагає спеціальних знань, тому складно навчити персонал.	- недостатня відмінність між важливими ризиками; - важко виправдати інвестиції в контроль реалізації, тому що немає підстав для аналізу витрат і переваг; - результати залежать від якості команди управління ризиками, яка буде створена

Взаємозв'язок між методами виявлення атак і методиками оцінки ризиків представлено на рис. 1.

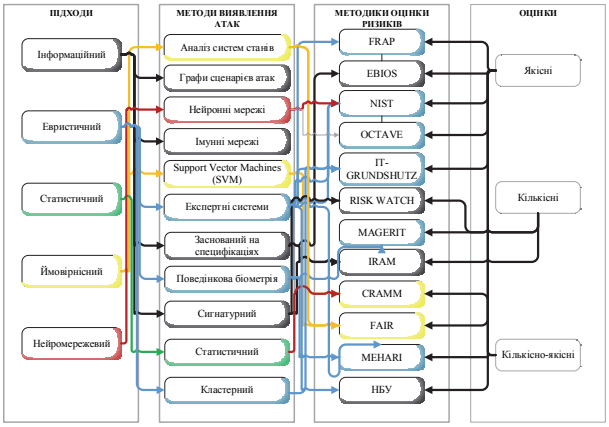

Рис. 1. Взаємозв'язок між методами виявлення атак та методиками оцінки ризиків

Комбінація кількісного і якісного методу являє собою змішану сукупність переваг і недоліків вище згаданих методів. З огляду різної природи загроз до профілів забезпечення комп'ютерної системи, розглянемо деякі методики оцінки ризиків (табл. 2).

Таблиця 2

Методики оцінки ризиків

Методика оцінки	Переваги	Недоліки	Підходи
NIST	- Детальний опис можливих ризиків інформаційних активів - Для підприємств різного розміру	- Довготривалий процес аналізу - Деякі функції не автоматизовано	Евристичний
FAIR	- Комплексний аналіз - Висока ефективність	- Для крупних підприємств	Ймовірнісний
IT-Grundshutz	- Гнучкість методу надає змогу проводити аналіз для будь-якої організації - Налаштовується на нові або існуючі активи	- Потребує теоретичної обізнаності процесу аналізу ризиків - Висока вартість ліцензії	Евристичний
CRAMM	- Детальне визначення існуючих ризиків - Ефективність використання	- Важкість у розумінні - Робота тільки з існуючими інф. активами	Ймовірнісний
OCTAVE	- Швидке впровадження - Обслуговує малі та середні за розміром підприємства	- Відсутність автоматизації - Не враховує специфіку банківської сфери	Евристичний
IRAM	- Відносна простота впровадження - Легкість в експлуатації	- Робота тільки з існуючими інформаційними активами	Інформаційний
EBIOS	- Велика кількість користувачів - Генерація звітів	- Лише для комерційних та державних установ	Інформаційний
RISK WATCH	- Простота впровадження та експлуатації	- Аналіз ризиків лише на програмно-технічному рівні	Інформаційний
MEHARI	- Формує оптимальну множину контрзаходів	- Застосовуваний до систем побудованих тільки за стандартом ISO	Евристичний
MAGERIT	- Систематичний метод аналізу - Кількісна оцінка - Гнучкість	- Результуючі дані залежать від людського фактору	Евристичний

У табл. 3 наведені результати досліджень деяких методик оцінки ризиків.

Таблиця 3

Результати досліджень методик оцінки ризиків

Методика	Атрибути							
	Якісна оцінка	Кількісна оцінка	Комплексна оцінка	Країна походження	Застосування у БС	Програмна реалізація	Ефективність контр-заходів	Простота розуміння
NIST	+			США	+	+	-	-
FAIR			+	США			+	+
EBIOS	+			Франція	+	+	+	-
MEHARI			+	Франція				
OCTAVE	+			США	+			
IT-GRUNDSHULTZ	+			Німеччина			+	
IRAM	+			Європа				+/-
RISK WATCH		+		США	+	+	+	+
FRAP	+			США				
CRAMM			+	Великобританія	+	+	+/-	+/-
MAGERIT	+	+		Іспанія	+	+		

В інтересах отримання в подальшому оцінок величини ризику еквівалентного грошового капіталу, та безпосереднього відображення її захищеності пропонується використовувати методики, засновані на комплексному підході до оцінки ризиків, що поєднує кількісні та якісні методи аналізу, до таких відносяться методики CRAMM і FAIR, структурні схеми наведені на рис. 2, 3 відповідно.

Рис. 2. Методика CRAMM – комплексний підхід до оцінки ризиків

Методики комплексного підходу оцінки ризиків, як правило, використовують такі стадії (етапи) [7; 17]:

на *першій стадії* аналізується все, що стосується ідентифікації та визначення цінності ресурсів системи: визначення меж досліджуваної системи: відомості про конфігурацію системи, відомості про відповідальних особах за фізичні і програмні ресурси, визначення кількості користувачів системи, їх привілеїв. Проводиться ідентифікація ресурсів: фізичних, програмних і інформаційних, що містяться всередині кордонів системи. Будується модель інформаційної системи з позиції ІБ;

на *другій стадії* ідентифікуються загрози і оцінюються рівні загроз для груп ресурсів і їх вразливостей, оцінюються залежність призначених для користувача сервісів від певних груп ресурсів і існуючий рівень загроз і вразливостей, обчислюються рівні ризиків і аналізуються результати. Наприкінці стадії замовник отримує ідентифіковані і оцінені рівні ризиків для своєї системи;

третя стадія дослідження полягає в пошуку адекватних контрзаходів – пошук варіанту системи безпеки, найкращим чином задовольняє вимогам замовника. На цій стадії генерує кілька варіантів заходів протидії, адекватних виявленим ризикам і їх рівнями.

Комплексування двох якісного та кількісного підходів дозволить об'єднати переваги кожного із них, що надаються ними окремо, та при цьому відкриє можливості отримання необхідних характеристик для ефективної організації систем захисту. В подальшому пропонується використовувати методику FAIR, засновану на комплексному підході до оцінки ризиків, що поєднує кількісні та якісні методи аналізу.

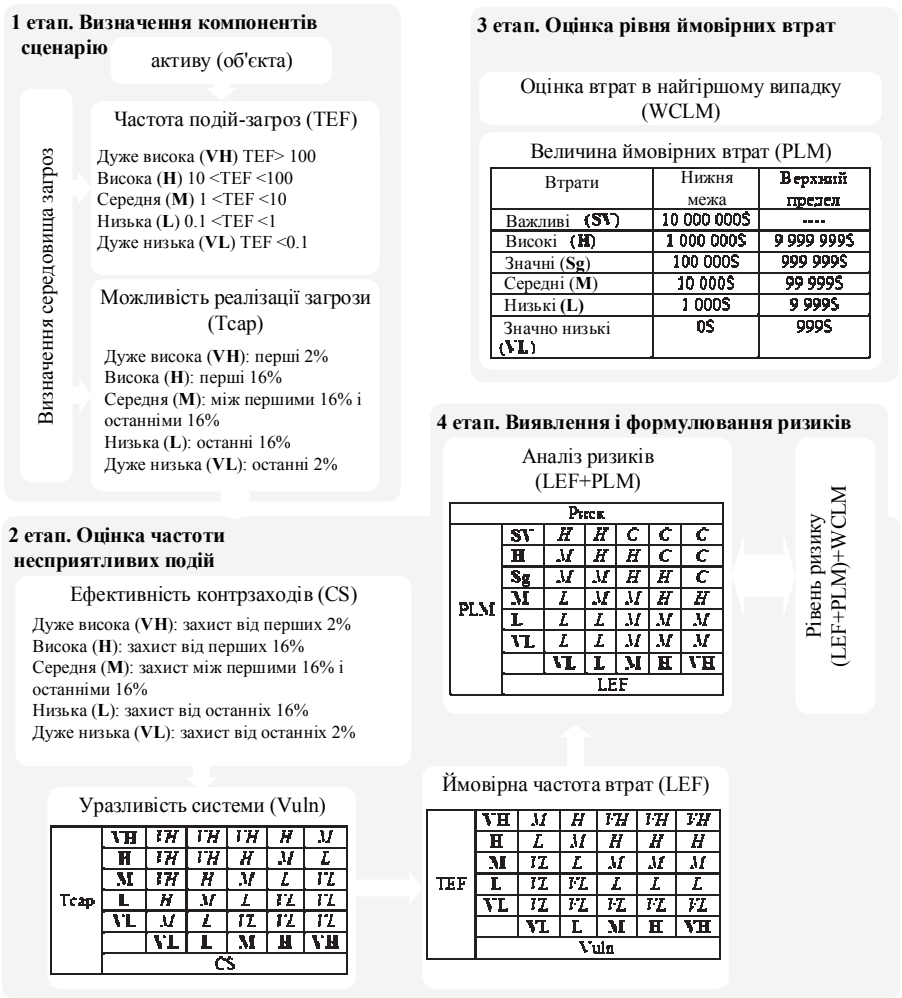

Рис. 3. Методика оцінки ризиків FAIR

2. Оцінка ризиків за методикою FAIR

Активи є об’єктом для багатьох видів загроз. Загроза може стати причиною небажаного інциденту, в результаті якого організації буде завдано шкоди. Цей збиток може виникнути в результаті атаки на інформацію, що належить організації і приводить до її несанкціонованого розкриття, модифікації, пошкодження, знищення, недоступності або втрати. Для кожного інформаційного активу або групи активів визначається список загроз щодо конфіденційності, цілісності та доступності. Оцінювання ри-

зиків полягає у визначенні їх кількісних і якісних значень, формуванні реєстру ризиків. Для того, щоб провести оцінку та аналіз ризиків, які впливають на активи підприємства, необхідно ідентифікувати активи.

На *першому etani*, визначаємо основні об'єкти(активи), на які впливають ризики, в області діяльності інформаційної безпеки організації та оцінюємо можливу частоту виникнення загроз (табл. 4).

У І півріччі 2016 року в світі оприлюднено і зареєстровано Аналітичним центром InfoWatch 840 випадків витоку конфіденційної інформації, що на 16% перевищує кількість витоків, зареєстрованих за аналогічний період 2015 року. В результаті витоків скомпрометовано 1,06 млн персональних даних.

Таблиця 4

Частота подій-загроз(TEF)

№	Опис параметра	∨	Значення
1	Дуже висока (VH)		>100
2	Висока (H)		10< TEF <100
3	Середня (M)	∨	1< TEF <10
4	Низька (L)		0.1< TEF <1
5	Дуже низька (VL)		<0.1

Проаналізувавши звіти великих компаній таких як, MCAfee Labs, Cisco та Infowatch, були виявлені групи активів та активи, котрі були використані в табл. 5.

Таблиця 5

Активи та групи активів організації

Активи/ частота загроз		**VH**	**H**	**M**	**VL**	**L**
Інформаційні активи	Бази даних	+				
	Файли		+			
	Документація					
	Заархівована інформація			+		
	Учбові матеріали					+
	Керівництво користувача				+	
Кадрові активи	Робітники університету			+		
Сервісні активи	Послуги моніторингу КС та усунення інцидентів	+				
	Моніторинг концентратів інформації				+	
	Моніторинг провайдерів		+			
	Внесення оновлень			+		
	Моніторинг локальних мереж та управління ними		+			
	Моніторинг та управління вузлами мережі передачі даних	+				
	Опалення					+
	Освітлення					+
	Сигналізація			+		
	Кондиціювання					+
Матеріальні активи	Послуга моніторингу		+			
	Апаратні засоби ІС	+				
	Сервери	+				
	Робочі станції		+			
	Принтери			+		
	Копіювальні апарати			+		
	Телекомунікаційне устаткування			+		
	Устаткування зв'язку		+			
	Маршрутизатори	+				
	Диски				+	
	Меблі					+
	Приміщення					+
	Виробниче устаткування			+		
	Технічні засоби			+		

Таким чином, аналіз табл. 5 показав, що частота виникнення загроз до активів університету – середня (M) від 1 до 10 разів на рік виникають загрози.

На *другому etani*, для оцінки частоти несприятливих подій використовуємо знання та досвід за допомогою зведених таблиць 6 – 9.

Таблиця 6

Ефективність контрзаходів(CS)

№	Опис параметра	∨	Захист
1	Дуже висока (VH)		Перших 2%
2	Висока (H)		Перших 16%
3	Середня (M)	∨	між першим 16% и останнім 16%
4	Низька (L)		Від останніх 16%
5	Дуже низька (VL)		останніх 2%

Таблиця 7

Можливість реалізації загрози (Tcap)

№	Опис параметра	∨	Значення
1	Дуже висока (VH)		перші 2%
2	Висока (H)		перші 16%
3	Середня (M)	∨	між першими 16% и останніми 16%
4	Низька (L)		останні 16%
5	Дуже низька (VL)		останні 2%

Визначимо уразливість активу (зусилля для отримання доступу – рівень захищеності активу). Для цього використовуємо значення, які визначили на другому етапі: можливості реалізації загрози – середня (M) та ефективність контрзаходів – середня (M). Результати наведені у табл. 8.

Таблиця 8

Уразливість системи (Vuln)

		Ефективність контрзаходів (CS)				
		VL	L	M	H	VH
Можливість реалізації загрози (Tcap)	VH	VH	VH	VH	H	M
	H	VH	VH	H	M	L
	M	VH	H	**M**	L	VL
	L	H	M	L	VL	VL
	VL	M	L	VL	VL	VL

Підставивши значення до табл. 8, визначимо уразливість активів до загроз – середня (M).

Далі визначимо частоту виникнення втрат (втрати конфіденційності активу), результати наведені в табл. 9.

Таблиця 9

Ймовірнісна частота витрат(LEF)

		Уразливість системи (Vuln)				
		VL	L	M	H	VH
Частота подій-загроз (TEF)	VH	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	**M**	M	M
	L	VL	VL	L	L	L
	VL	VL	VL	VL	VL	VL

Підставивши значення, отримаємо частоту виникнення втрат – середня (M).

На *третьому етапі*, визначимо втрати в найгіршому випадку (табл. 11), використовуючи табл. 10.

Таблиця 10

Величина ймовірних втрат (PLM)

№	Втрати	Нижня межа	Верхня межа
1	Серйозні (SV)	10 000 000	-
2	Високі (H)	1 000 000	9 999 999
3	Значні(Sg)	100 000	999 999
4	Середня (M)	10 000	99 999
5	Маленькі (L)	1 000	9 999
6	Гранично маленькі (VL)	0	999

Таблиця 11

Втрати в найгіршому випадку

	Інформаційні активи	Кадрові активи	Сервісні активи	Матер. активи
Доступ				
Неправильне вживання				
Розкриття	SV	H	-	H
Модифікація				
Відмова у доступі				

Визначимо величину можливих втрат, табл. 12.

Таблиця 12

Величина можливих втрат

	Інформаційні активи	Кадрові активи	Сервісні активи	Матеріальні активи
Доступ				
Неправильне вживання				
Розкриття	H	Sg	H	M
Модифікація				
Відмова у доступі				

На *четвертому етапі*, вимірюємо та формалізуємо ризик, табл. 13.

Таблиця 13

Формування ризиків

		Ймовірнісна частота витрат(LEF)				
		VL	L	M	H	VH
Величина ймовірних втрат (PLM)	SV	H	H	C	C	C
	H	M	H	**H**	C	C
	Sg	M	M	H	H	C
	M	L	M	M	H	H
	L	L	L	M	M	M
	VL	L	L	M	M	M

Аналіз результатів табл. 13 свідчить, що при розгляданні всіх активів, великі втрати несуть інформаційні та сервісні активи.

3. Дослідження ефективності передачі даних в комп'ютерних системах мережах при різних способах управління обміном даних

на основі алгоритму запропонованого авторами в роботах [5; 6; 20; 21].

Для підвищення значення показника функціональної ефективності комп'ютерної мережі використаємо такі 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).

Досліджуємо ГОМ, що використовують дані способи управління обміном даними. В якості вихідних даних виступають такі параметри:

а) параметри каналу передачі даних:

ймовірність помилки біта, $P_{пом}$;

пропускна здатність каналу передачі даних, C;

довжина лінії зв'язку, L;

швидкість поширення сигналу в середовищі Vp.

б) параметри комп'ютерної мережі:

довжина інформаційного кадру n;

довжина квитанції s (для систем зі зворотнім зв'язком);

кратність виявлення помилки r (для систем з виявленням помилок);

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

розмір вікна Z (для систем с ВЗЗбп "*Повернення-на-N*");

задана ймовірність доставки пакету РЗ (для систем с ВЗЗпк).

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

$$W(u_1) = \frac{n^{(u_1)} - t^{(u_1)}}{n^{(u_1)}} \frac{B^{(u_1)} - \Psi^{(u_1)}}{B^{(u_1)}} P_{пр\,п}{}^{(u_1)} W_{eff}, \quad (1)$$

$$t^{(u_1)} = \frac{n}{C} + \frac{L}{V_p} + t_{ш} + t_{рш}, \quad (2)$$

$$P_{пр\,п}^{(u_1)} = (1 - P_0)^n, \quad (3)$$

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

$$W(u_2) = \frac{n^{(u_2)} - t^{(u_2)}}{n^{(u_2)}} \frac{B^{(u_2)} - \Psi^{(u_2)}}{B^{(u_2)}} P_{пр\,п}{}^{(u_2)} W_{eff}, \quad (4)$$

$$t^{(u_2)} = \frac{n}{C} + \frac{L}{V_p} + t_{ш} + t_{рш}, \quad (5)$$

$$P_{пр\,п}^{(u_2)} = \sum_{i=0}^{t} C_n^i P_0^i (1 - P_0)^{n-i}, \quad (6)$$

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

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

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

$$+ \frac{\sum_{i=1}^{r} C_n^i \cdot P_0^i \cdot (1 - P_0)^{n-i} + (1 - \frac{1}{2^r}) \cdot \sum_{i=r+1}^{n} C_n^i \cdot P_0^i \cdot (1 - P_0)^{n-i}}{(1 - P_0)^n} \times \left(\frac{n+s}{C} + 2\frac{L}{V_p}\right), \quad (8)$$

$$P_{пр\,п}^{(u_3)} = \frac{(1 - P_0)^n}{1 - \sum_{i=1}^{r} C_n^i P_0^i (1 - P_0)^{n-i} - (1 - \frac{1}{2^r}) \cdot \sum_{i=r+1}^{n} C_n^i P_0^i (1 - P_0)^{n-i}}, \quad (9)$$

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

$$W(u_4) = \frac{n^{(u_4)} - t^{(u_4)}}{n^{(u_4)}} \frac{B^{(u_4)} - \Psi^{(u_4)}}{B^{(u_4)}} P_{пр\,п}{}^{(u_4)} W_{eff}, \quad (10)$$

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

$$+ \frac{\sum_{i=1}^{r} C_n^i \cdot P_0^i \cdot (1 - P_0)^{n-i} + (1 - \frac{1}{2^r}) \cdot \sum_{i=r+1}^{n} C_n^i \cdot P_0^i \cdot (1 - P_0)^{n-i}}{(1 - P_0)^n} \cdot \frac{n}{C}, \quad (11)$$

$$P_{\text{пр п}}^{(u_4)} = (1-P_0)^n \frac{1-\left(\sum_{i=1}^{r} C_n^i P_0^i (1-P_0)^{n-i} + (1-\frac{1}{2^r})\cdot \sum_{i=r+1}^{n} C_n^i P_0^i (1-P_0)^{n-i}\right)^N}{1-\sum_{i=1}^{r} C_n^i P_0^i (1-P_0)^{n-i} - (1-\frac{1}{2^r})\cdot \sum_{i=r+1}^{n} C_n^i P_0^i (1-P_0)^{n-i}}, \quad (12)$$

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:

а) в комп'ютерної мережі, що використовує циклічні коди в режимі виявлення помилок, значення показника ефективності визначається як [8; 16; 20; 21]:

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

б) для комп'ютерної мережі без зворотного зв'язку при виправленні t-кратної помилки циклічним кодом, значення показника ефективності визначається як [8; 16; 20; 21]

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

в) для комп'ютерної мережі з вирішальним зворотним зв'язком і безперервним передаванням кадрів "Повернення-на-N" значення показника ефективності визначається як [8; 16; 20; 21]:

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

г) для комп'ютерної мережі з вирішальним зворотним зв'язком і позитивною квитанцією кадрів значення показника ефективності визначається як [8; 16; 20; 21]:

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

На рис. 4 наведені результати дослідження відповідних стратегій в каналах передачі без пам'яті за допомогою виразів (13–16).

Позначення:

1 – Повернення-на-N (протокол із симетричною криптосистемою) для *Ethernet 10 Gb*;

2 – Састрі (з вирішальним зворотним зв'язком) (протокол із симетричною криптосистемою) для *Ethernet 10 Gb*;

3 – Повернення-на-N для *Ethernet 40 Gb*;

4 – Састрі для *Ethernet 40 Gb*;

Примітка:

$C_1 = 10^9$ біт/с; $C_2 = 4\times10^9$ біт/с; L = 1000 км; Vp = $3\cdot10^8$ м/с; t = 8; n = 1518; k = 16; $P_{\text{зад}} = 0{,}95$; $t_{\text{ш\_сим}} = t_{\text{расш\_сим}} = 0{,}01$ с; $t_{\text{ш\_асим}} = t_{\text{расш\_асим}} = 10^2$ с; $B = 10^{24}$; $\Psi = 10^{15}$; $\text{Econ}_{10\text{GB}} = 31.45$; $\text{Econ}_{40\text{GB}} = 19.66$.

Аналіз результатів, наведених на рис. 1, 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 $P_{\text{пом}} = 10^{-3} – 10^{-2}$, та збільшення якості обслуговування клієнтів за рахунок використання технологій *Ethernet 40 Gb*.

Детальне дослідження статистичних властивостей послідовностей помилок в реальних каналах зв'язку [2] показало, що помилки залежні та мають тенденцією до скупчення (пакетування), тобто між ними існує певна залежність – кореляція.

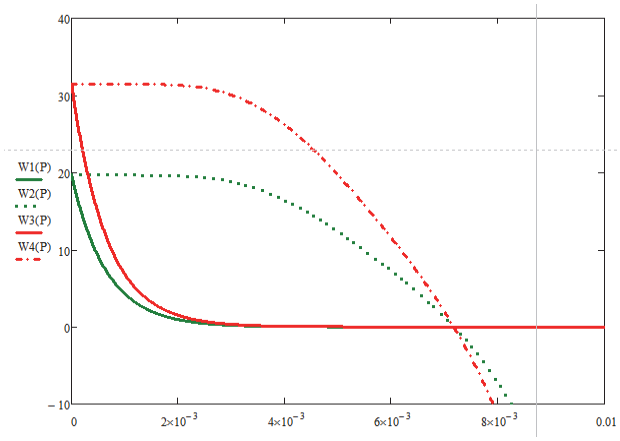

Рис. 4. Показник функціональної ефективності в каналах без пам'яті

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 $P_{\text{пом}}$ необхідно задати наступні чотири канальних параметри:

ймовірність виникнення пакету помилок $P_{пом}$;

ймовірність помилки усередині пакету дорівнює P_{ε};

математичне сподівання mln довжини пакету помилок;

середньоквадратичне відхилення σln довжини пакету помилок.

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

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

$$W(u_1) = \frac{n^{(u_1)} - t^{(u_1)}}{n^{(u_1)}} \frac{B^{(u_1)} - \Psi^{(u_1)}}{B^{(u_1)}} P_{\text{пр п}}{}^{(u_1)} W_{eff}\ , \tag{17}$$

$$t^{(u_1)} = \frac{n}{C} + \frac{L}{V_p} + t_{ш} + t_{рш}\ , \tag{18}$$

$$P_{\text{пр п}}^{(u_1)} = 1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_{п})^{n+i} \right] \left[\Phi\left(\frac{i + 1 - m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i - m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}. \tag{19}$$

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

$$W(u_2) = \frac{n^{(u_2)} - t^{(u_2)}}{n^{(u_2)}} \frac{B^{(u_2)} - \Psi^{(u_2)}}{B^{(u_2)}} P_{\text{пр п}}{}^{(u_2)} W_{eff}\ , \tag{20}$$

$$m_t^{(u_2)} = \frac{n}{C} + \frac{L}{V_p} + t_{ш} + t_{рш}\ , \tag{21}$$

$$P_{\text{пр п}}^{(u_2)} = 1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_{п})^{n-t+i} \right] \left[\Phi\left(\frac{i + 1 - m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i - m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}, \tag{22}$$

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

$$W(u_3) = \frac{n^{(u_3)} - t^{(u_3)}}{n^{(u_3)}} \frac{B^{(u_3)} - \Psi^{(u_3)}}{B^{(u_3)}} P_{\text{пр п}}{}^{(u_3)} W_{eff}\ , \tag{23}$$

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

$$+ \frac{\sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_{п})^{n+i} \right] \cdot \left[\Phi\left(\frac{i + 1 - m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i - m_{l_n}}{\sigma_{l_n}} \right) \right] \right\} \left\{ 1 - \frac{1}{2^r} \left[\frac{1}{2} - \Phi\left(\frac{r + 1 - m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}}{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_{п})^{n+i} \right] \left[\Phi\left(\frac{i + 1 - m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i - m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}} \times \tag{24}$$

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

$$P_{\text{пр п}}^{(u_3)} = \frac{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_{п})^{n+i} \right] \left[\Phi\left(\frac{i + 1 - m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i - m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}.}{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_{п})^{n+i} \right] \left[\Phi\left(\frac{i + 1 - m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i - m_{l_n}}{\sigma_{l_n}} \right) \right] \right\} \left\{ 1 - \frac{1}{2^r} \left[\frac{1}{2} - \Phi\left(\frac{r + 1 - m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}} \tag{25}$$

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

$$W(u_4) = \frac{n^{(u_4)} - t^{(u_4)}}{n^{(u_4)}} \frac{B^{(u_4)} - \Psi^{(u_4)}}{B^{(u_4)}} P_{\text{пр п}}^{(u_4)} W_{\text{eff}}, \quad (26)$$

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

$$\frac{\sum_{i=0}^{\infty}\left\{\left[1-(1-P_{\text{п}})^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\left\{1-\frac{1}{2^r}\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_{\text{п}})^{n+i}\right]\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}, \quad (27)$$

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

$$\frac{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_{\text{п}})^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\left\{1-\frac{1}{2^r}\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}^N}{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_{\text{п}})^{n+i}\right]\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\left\{1-\frac{1}{2^r}\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}, \quad (28)$$

В результаті розрахунків за допомогою виразів (17; 20; 23; 26) отримано числові значення показника ефективності комп'ютерної мережі W при зміні ймовірності виникнення пакету помилок $P_{\text{пом}}$.

На рис. 2 наведені результати дослідження відповідних стратегій в дискретних каналах передачі з пам'яттю за допомогою виразів (17; 20; 23; 26). Позначення:1 – Повернення-на-N (протокол із симетричною криптосистемою) для *Ethernet 10 Gb*; 2 – Састрі (з вирішальним зворотним зв'язком) (протокол із симетричною криптосистемою) для *Ethernet 10 Gb*; 3 – Повернення-на-N для *Ethernet 40 Gb*; 4 – Састрі для *Ethernet 40 Gb*;

$C_1 = 10^9$ біт/с; $C_2 = 4\times10^9$ біт/с; L = 1000 км; Vp = $3\cdot10^8$ м/с; t = 8; n = 1518; k = 16; $P_{\text{зад}} = 0{,}95$; $t_{\text{ш\_сим}} = t_{\text{расш\_сим}} = 0{,}01$ с; $t_{\text{ш\_асим}} = t_{\text{расш\_асим}} = 10^2$ с; $B = 10^{24}$; $\Psi = 10^{15}$; $\text{Econ}_{10\text{GB}} = 31.45$; $\text{Econ}_{40\text{GB}} = 19.66$.

Аналіз результатів рис. 2 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. 4–5 демонструє, що застосування несиметричних криптосистем знижує вимоги з оперативності – час формування пакету даних зростає на 20%, компенсацією цього можливе використання технологій *Ethernet 10 Gb, Ethernet 40 Gb*.

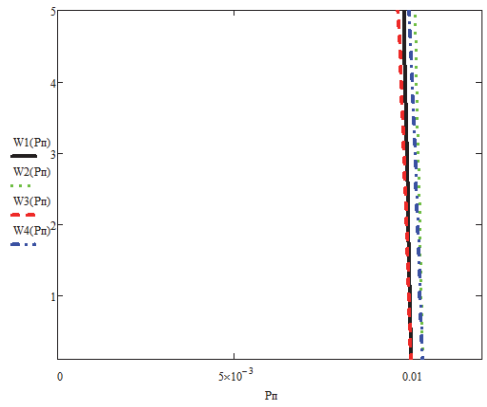

Рис. 5. Показник функціональної ефективності в каналах с пам'яттю

Висновки

Для проведення дослідження був введений узагальнений показник ефективності комп'ютерної мережі (W_i). При цьому були досліджені залежності коефіцієнта готовності від довжини кадру, часу доставки кадру при різних ймовірностях помилки в каналі передачі з використанням асиметричних та симетричних алгоритмів шифрування. Для дослідження були використані різні стратегії управління обміном даних. У результаті дослідження було виявлено, що на коефіцієнт готовності істотно впливає довжина кадру (оперативність), час шифрування та розшифрування (безпека), ймовірність помилки (надійність). При чому збільшення довжини кадру є причиною збільшення ймовірності помилки, що призводить до зниження коефіцієнта готовності. В цифрових каналах ймовірність помилки є низькою і її використання призводить до збільшення коефіцієнта готовності, що є практичним результатом. Також алгоритми шифрування неіс-

тотно впливають на оперативність, тому що збільшується продуктивність обчислювальних технологій та систем на основі закону Мура.

Проведене дослідження показало, що для забезпечення ефективності узагальненого показника необхідно використовувати довжини пакетів стандартів фізичного рівня (стандарт IEEE.802.X) та канали зв'язку UTP5, СТР, оптоволоконні кабелі, які забезпечують ймовірність помилки 10^{-8} – 10^{-12}. Стратегії з вирішальним зворотним зв'язком і безперервною передачею кадрів "Повернення-на-N" та з вирішальним зворотним зв'язком і позитивною квитанцією є найкращими на основі каналів з пам'яттю та без пам'яті та показують необхідні показники.

Список літератури

1. ISO 9000:2005. Системы менеджмента качества. Основные положения и словарь [Електронний ресурс]: – Режим доступу: https://www.iso.org/obp/ui#iso:std:iso:9000:ed-3:v1:ru.

2. Астрахов А.М. Искусство управления информационными рисками / А.М. Астрахов. – М.: ДМК Пресс, 2010. – 312 с.

3. 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.

4. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity [Електронний ресурс]: – Режим доступу до ресурсу: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375.

5. Евсеев С.П. 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.

6. Евсеев С.П. 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.

7. Захист інформації та економічна безпека підприємства: монографія / О.О. Кузнецов, С.П. Евсеев, С.В. Кавун. – Харків: Вид. ХНЕУ, 2008. – 360 с.

8. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

9. 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.

10. Концепция создания системы контроля качества предоставления услуг связи в Российской Федерации [Електронний ресурс]: – Режим доступу: http://minsvyaz.ru/ru/documents/4668/.

11. Луцкий М.Г. Базовые понятия управления риском в сфере информационной безопасности / М.Г. Луцкий, Е.В. Иваненко // Защита информации. – 2011. – №2. – С. 86-94.

12. Макаревич Л.М. Управление предпринимательскими рисками: монография / Л.М. Макаревич. – М. : Дело и Сервис, 2006. – 443 с.

13. МСЭ-Т G.1011 Справочное руководство по существующим стандартам методик определения оценки пользователем качества услуги (QoE). [Електронний ресурс]: – Режим доступу: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11931&lang=ru.

14. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи : ДМК Пресс, 2004. – 384 с.

15. Семенов С.Г. 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.

16. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.; пер. с англ. / Б. Скляр. – М.: Издательский дом "Вильямс", 2003. – 1104 с.

17. Смірнов О.А. Технології і стандарти комп`ютерних мереж. / О.А. Смірнов, С.П. Евсеев, В.Ю. Жукарев, О.Г. Король, В.Є. Сорокін, Є.В. Мелешко. – Д.: ДонІЗТ, 2012. – 453 с.

18. Стандарт ГОСТ РВ 51987 «Информационная технология, комплекс стандартов на АС» [Електронний ресурс]: – Режим доступу: http://gearletitbit.weebly.com/blog/gost-rv-51987-2002.

19. Степаненко Е.В. Использование метрологических принципов для оценки эффективности работы инфокоммуникационных систем и сетей // Психолого-педагогический журнал Гаудеамус, № 2 (16). – 2010. – С. 1-4.

20. Сумцов Д.В. Загальний показник ефективності передачі даних у комп'ютерній мережі / Д.В. Сумцов, Б.П. Томашевський // Системи обробки інформації. – Х.: ХУПС, 2009.

21. Сумцов Д.В. Общий показатель эффективности передачи данных в компьютерной сети / Д.В. Сумцов, Б.П. Томашевский, А. . Носик // Системи обробки інформації. – Х.: ХУПС, 2009. – Вип. 7(79). – С. 85-90.

Надійшла до редколегії 6.03.2017

Рецензент: д-р фіз.-мат. наук проф. С.Є. Остапов, Чернівецький національний університет імені Юрія Федьковича, Чернівці.

ОЦЕНКА КАЧЕСТВА ОБСЛУЖИВАНИЯ ГЛОБАЛЬНОЙ СЕТИ НА ОСНОВЕ ТЕХНОЛОГИЙ ETHERNET С ПОМОЩЬЮ КОМПЛЕКСНОГО ПОКАЗАТЕЛЯ

О.Г. Король

В статье проведена оценка качества обслуживания пользователей глобальной вычислительной сети Ethernet на основе комплексного показателя, объединяющего технические и экономические показатели. На основе анализа методик оценки экономического ущерба (методики оценки рисков) для проведения интегрированной оценки качества обслуживания предлагается использовать методику Fair, что позволяет получить как качественный, так и количественный показатель ущерба.

Ключевые слова: *комплексный интегрированный показатель качества обслуживания, методика оценки ущерба (риска), глобальные сети Ethernet.*

EVALUATION OF THE QUALITY OF SERVICE TO A GLOBAL NETWORK BASED ON ETHERNET TECHNOLOGY THROUGH A COMPREHENSIVE INDEX

O. Korol

In the article the user experience evaluation of the global Ethernet computer network in an integrated index, which brings together the technical and economic indicators. Based on the analysis of economic losses (risk assessment procedures) assessment methodologies for integrated assessment of the quality of service offered to use methodology Fair, to provide both qualitative and quantitative measure of damages.

Keywords*: complex integrated indicator of quality of service, damage assessment methodology (risk), global Ethernet network.*