УДК 004.7:004.94(045)

Зубарева О. О.,
Шевцова Є. В.,
Безвершенко Є. І.

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ГАРАНТОВАНОЇ ЯКОСТІ ОБСЛУГОВУВАННЯ ТРАФІКУ КОМП'ЮТЕРНИХ МЕРЕЖ

Національний авіаційний університет

Проаналізовано методи забезпечення якості обслуговування трафіку у комп'ютерних мережах. Запропоновано застосування критерію захищеності як додаткового параметру гарантованої якості обслуговування у комп'ютерних мережах

Вступ

Технологія комп'ютерних мереж наступного покоління *(NGN)* вимагає забезпечення гарантованої якості обслуговування *(QoS)*. Визначення показників *QoS* в значній мірі базується на експертних оцінках. Мережі з комутацією пакетів мають механізми забезпечення *QoS* в процесі експлуатації.

Питання забезпечення *QoS* в ком'ютерних мережах КМ розглядалися в роботах багатьох вчених, зокрема Е.А. Кучерявого, Ю.А. Семенова, Ю.В. Семенова та інш. Результати досліджень можуть бути застосовані для визначення характеристик *QoS* [1].

Побудова розподілених інфокомунікаційних систем вимагає гарантоздатності телекомунікаційних систем та комп'ютерних мереж при дії деструктивних чинників (відмови, завади, атаки на мережу та інших). Гарантоздатність характеризує ступінь працездатності системи на будь-якому інтервалі часу функціонування за умови її справності в початковий момент.

Мета дослідження

Метою роботи є параметричне дослідження важливих показників *QoS:* надійності функціонування та захищеності інформації КМ. Існує велика кількість матеріалів по рішенню окремих проблем цієї тематики, але залишаються актуальними та вимагають детального розгляду та доопрацювання питання *QoS* мультимедійного трафіку.

Виклад основних матеріалів дослідження

Основні показники забезпечення гарантованої якості обслуговування мультимедійного трафіку наведені на рис. 1.

При передачі мультимедійних даних для забезпечення потрібного рівня *QoS* необхідно враховувати основні характеристики:

– загальну оцінку якості передачі;

– якість передачі мультимедійного трафіку;

– затримку передачі даних;

– показники надійності функціонування КМ

– захищеність інформації в КМ.

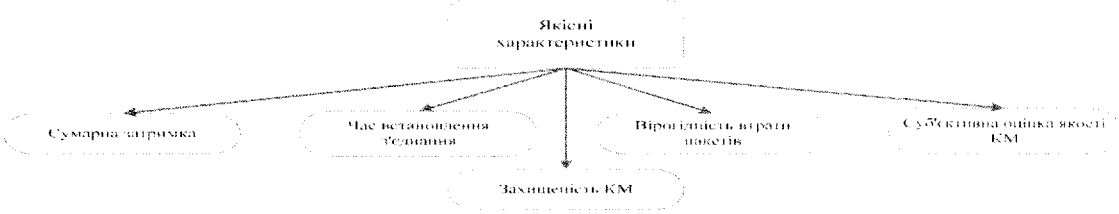


Рис.1. Основні показники забезпечення *QoS* мультимедійного трафіку.

Надійність функціонування комп'ютерних та телекомунікаційних мереж характеризується, у першу чергу, ступенем зв'язку вузлів комутації (ВК) з мережею і обумовлена заданим числом

ліній зв'язку (ЛЗ) l_i. При формуванні топології мережі головними умовами є:

- забезпечення необхідної зв'язності кожного ВК із іншими ВК мережі;
- забезпечення заданої інтенсивності реконфігурації топології мережі за рахунок відновлення ЛЗ у випадку появи збоїв.

Процес функціонування мережі залежить від інтенсивності збоїв та інтенсивності відновлення ЛЗ. Параметр відновлення повинен значно перевищувати інтенсивності збоїв. Якщо ця вимога не виконується, то відбувається процес повної деградації мережі.

На сьогоднішній день при побудові мереж застосовуються класичні топології: «зірка», «кільце», «коміркова», «повна сітка». На рис. 2 представлена мережа з п'ятьма ВК, що має топологію «кільце» (рис. 2а) та «повна сітка» (рис. 2б).

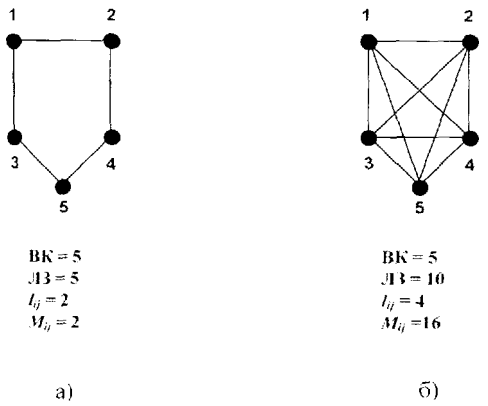


Рис. 2. Варіанти топології мережі з п'ятьома ВК: *а* – «кільце», *б* – «повна сітка»

З точки зору відмовостійкості найбільш ефективною є топологія «повна сітка».

Розглянемо ймовірності моделі функціонування КМ. Під ймовірністю ефективного функціонування мережі розуміють ймовірність перебування мережі в працездатному стані (із заданим числом зв'язків ВК із мережею). Іншими словами, мережа повинна бути цілою, а не розпадатися на окремі сегменти. Виділивши два стохастичних процеси надходження мультимедійного трафіку (ММТ) у різні моменти часу на різні ВК і відмову ЛЗ обчислимо оцінку ефективності функціонування мерсжі $P_{еф}(t, \Delta t)$ [2, 4]:

$$P_{эф}(t,\Delta t) = P_{нф}(t,\Delta t) * P_{эп}(t,\Delta t_{пер}), \qquad (1)$$

де $P_{еф}(t,\Delta t)$ – ймовірність ефективного функціонування мережі; $P_{нф}(t, \Delta t)$ – ймовірність нормального функціонування ВК мережі протягом часу Δt; $P_{еп}(t, \Delta t_{пер})$ – ймовірність передачі ММТ із заданою якістю обслуговування протягом часу $\Delta t_{пер}$.

$$P_{еп} = e^{-\frac{\Delta t}{T_{бп}}}, \qquad (2)$$

де $T_{бп}$ – середній час безпомилкової передачі.

Виходячи з вимог підтримки заданого рівня відмово стійкості (нормального функціонування мерсжі), щоразу після виникнення збою, формується нова топологія мережі, яка забезпечує необхідну зв'язність ВК. При такому підході можна дати оцінку стійкості до збоїв з урахуванням забезпечення своєчасності передачі ММТ [5]. При цьому ступінь зв'язності l кожного ВК із мережею характеризує зв'язність комп'ютерної мережі вцілому. Наприклад, якщо всі ВК мають не менше двох зв'язків із мережею ($l \geq 2$), то вважається що така мережа перебуває в режимі нормального функціонування. Якщо ж є ВК, у якого залишився лише один зв'язок з мережею ($l = 1$), то наступає режим критичного функціонування.

Вважаючи появу збоїв і відновлення кожної ЛЗ як незалежні процеси, а деградацію мережі – як критичний випадок, що виник у процесі передачі ММТ, можна дати оцінку станам стійкості мережі: події нормального, критичного та ненормального функціонування. При відомому часі знаходження мережі в кожному із цих станів, можна визначити ймовірність нормального функціонування мережі [2]:

$$P_{нф}(t,\Delta t) = K_{гс}(t) * P_{нп}(\Delta t), \qquad (3)$$

де $K_{гм}(t)$ – коефіцієнт готовності мережі. Він вказує на ймовірність застати мережу *будь-який момент часу в станах із заданою* зв'язністю ВК (наприклад, $l \geq 2$);

$P_{пт}(\Delta t)$ – ймовірність надійної стійкості передачі ММТ із заданою якістю обслуговування у мережі протягом часу Δt.

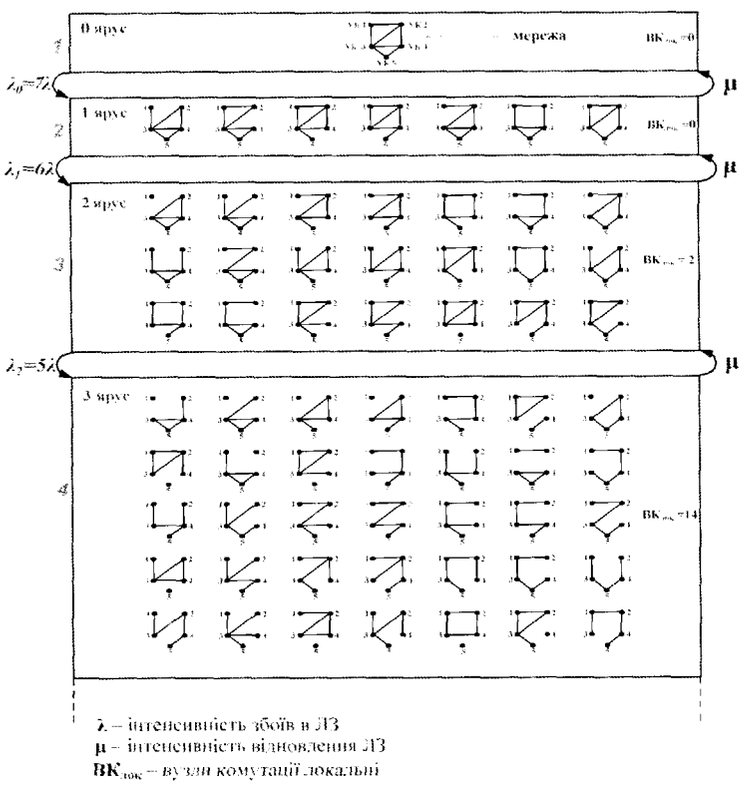
Розглядаючт випадок, коли $1 << \frac{\mu_в}{n\lambda_с}$,

(n – число ЛЗ в мережі, $\lambda_с$ – інтенсивність появи збоїв у кожній ЛЗ та $\mu_в$ – інтенсивність відновлення ЛЗ) можна припустити, що $P_{нп}(\Delta t) \approx 1$. Тоді вираз (3) приймає вигляд:

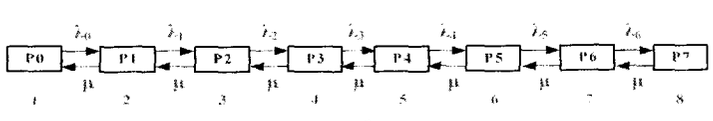
$$P_{нф}(t,\Delta t) \approx K_{гс}(t) \quad . \qquad (4)$$

Процес деградації розглянемо на прикладі стільника з п'ятиранговою топологією та сімома ЛЗ. На рис. 3 у вигляді графів переходів представлені дві базові формальні моделі деградації мережі: поярусова (а) [2, 6], та «загибелі та розмноження» (б) [8].

Яруси – це працездатні стани мережі, які об'єднані у відповідні групи за ознакою відмов ЛЗ, що зменшують для кожного ВК кількість зв'язків з мережею.



а



б

Рис. 3. Моделі функціонування п'ятирангової мережі:
а – поярусна, *б* – «загибелі та розмноження»

Число сполучень з n елементів по m C_n^m визначається по по формулі:

$$C_n^m = \frac{n!}{(n-m)!\cdot m!}, \qquad (5)$$

де n – загальна кількість ЛЗ в мережі,; m – кількість ЛЗ на k-ому ярусі, що відмовили.

На нульовому ярусі всі ЛЗ знаходяться в функціональному стані, вони мають один працездатний стан $C_9^0 = 1$, $\min l \geq 2$, для кожної ЛЗ. На першому ярусі всі ЛЗ працездатні ($C_9^1 = 1$, зв'язність $\min l \geq 2$). Це режим нормального функціонування. На другому ярусі – як і на попередніх , всі ЛЗ є справними (число станів $C_9^2 = 36$, при зв'язності $\min l \geq 1$). Це режим нормального функціонування мережі. Третій ярус – відмовило сім ЛЗ (число ста-

ній $C_9^3 = 84$, з них один стан являє собою окремі сегменти мережі, а шість ВК стали окремими з мінімальною зв'язністю $l = 0$). Коефіцієнт зв'язності $K_{ся}$ (при $\min l \geq 1$) можна розрахувати за формулою [3]:

$$K_{ся}^{l\geq 1} = \frac{M_я - M_{лок}}{M_я} = \frac{84-7}{84} = 0{,}917, \quad (6)$$

де $M_я$ – загальна кількість станів ярусу; $M_{лок}$ – кількість станів на ярусі із локальними ВК.

Відповідно, коефіцієнт втрати зв'язності третього ярусу $K_{пся}^{l\geq 1}$ дорівнює:

$$K_{пся}^{l\geq 1} = \frac{M_{лок}}{M_я} = \frac{7}{84} = 0{,}083. \quad (7)$$

Це режим критичного функціонування з погляду забезпечення зв'язності, тому що існують ВК зв'язність яких $l = 0$. Ймовірність локалізації ВК відносно мала ($P_{лок}$= 0,083).

Четвертий ярус – блоковано п'ятдесят дві ЛЗ (число станів $C_9^4 = 126$, з них 60 станів не є цільною зв'язною мережею, а тридцять шість ВК стали локальними з мінімальною зв'язністю $l = 0$). Для даного ярусу коефіцієнт зв'язності $K_{ся}$(при $l \geq 1$) буде дорівнювати $K_{ся}^{l\geq 1} = \frac{126-52}{126} = 0{,}587$. Відповідно, коефіцієнт втрати зв'язності цього ярусу $K_{пся}^{l\geq 1}$ складе: $K_{пся}^{l\geq 1} = \frac{52}{126} = 0{,}413$. Таким чином, на четвертому ярусі ймовірність локалізації ВК становить $P_{лок} = 0{,}413$. Це режим ненормального функціонування мережі (зрив передачі ММТ).

Алгоритм поярусного відбору критичних станів у процесі деградації комп'ютерної мережі

У роботі [1] розглянуто питання формування алгоритму поярусного відбору критичних станів.

В основу алгоритму поярусного відбору покладений принцип циклічного формування значень $K_{гс}$ для отримання залежності фоефіцієнта готовності мережі від інтенсивності виникнення збоїв. Аналіз працездатності проводиться з врахуванням наступних параметрів:

- топології мережі (з певною кількістю ВК $N_{ВК}$ і заданою кількістю ЛЗ $N_{ЛЗ}$);
- ступеня зв'язності ВК із мережею $l \geq l_{тр}$;
- інтенсивності зниження працездатності ЛЗ між ВК мережі за рахунок появи збоїв $\lambda_с$;
- інтенсивності відновлення ЛЗ $\mu_в$.

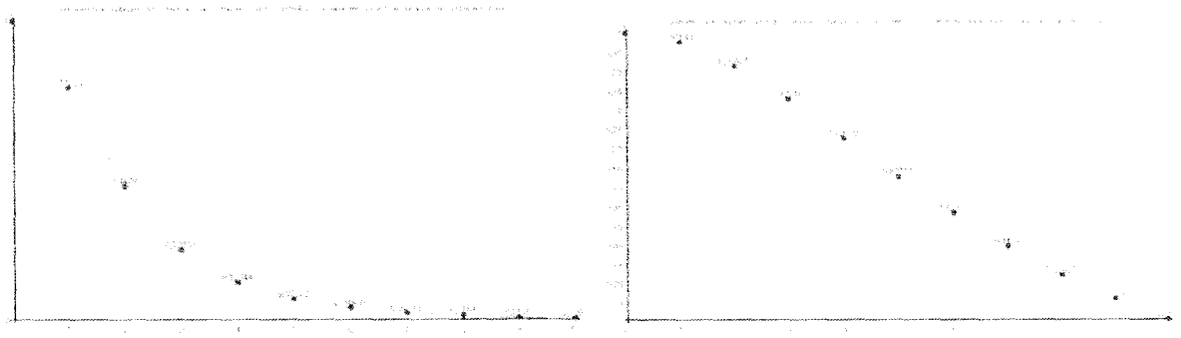
Далі для кожної топології мережі, інтенсивності появи збоїв $\lambda_с$ і необхідного ступеня зв'язності ВК із мережею ($l = 1$) *проводиться розрахунок* $K_{гм}$ для обраних опорних значень інтенсивності відновлення ЛЗ $\mu_{в_{min}}$ та $\mu_{в_{max}}$, відбираються значення парметрів $\mu_в$, при яких виконується умова $K_{гм} \geq K_{потр}$. Наприклад, для $K_{гм} \geq 0{,}95$ за результатами порівняльного аналізу обирається найбільш прийнятна топологія стільника з урахуванням ступеня зв'язності $l_{потр}$, а також значення $\mu_в$, які відповідають вище зазначеній умові.

Програмні засоби моделювання представлені у вигляді програмного модуля, реалізованого в середовищі *Delphi*.

На рис. 4 представлені результати моделювання процесу повної деградації мережі з п'ятьма ВК та різними топологіями («кільце» та «повна сітка»).

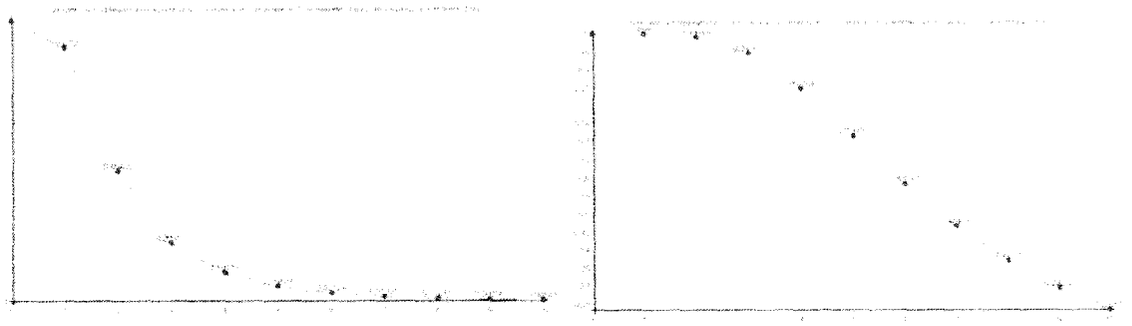
Аналіз ефективності відновлення ЛЗ (реконфігурації топології мережі) у вигляді графіків залежності коефіцієнта готовності $K_{гм}$ від інтенсивності появи збоїв при заданому критерії зв'язності $l \geq 1$ і двох режимах відновлення $\mu_в$=0,4, $\mu_в$=1,4 для топології «кільце» наведено на рис. 4.

Працездатність мережі цілком залежить від інтенсивності відновлення ЛЗ, що забезпечує необхідну стійкість мережі до виникнення збоїв (наприклад при зв'язності $l_{ij} \geq 1$ $K_{гс} \geq 0{,}95$ у межах інтенсивності збоїв $\lambda_з$ = 0÷0,0075 (рис.4.б)). При підвищенні ступеня зв'язності ВК із мережею (рис.5.б) і $\mu_в = 1{,}4$ для умови $l_{ij} = 1$ вдається підтримати працездатність мережі вже для більших значень інтенсивності збоїв до $\lambda_з = 0{,}05$.



а *б*

Рис. 4. Графік залежності коефіцієнта готовності з п'ятьма ВК і топологією «кільце» від інтенсивності збоїв ($\lambda_з$ = 0,05 для критерію зв'язності $l \geq 1$): *а*) $\mu_в$ = 0,4; *б*) $\mu_в$ = 1,4.



а *б*

Рис. 5. Графік залежності коефіцієнта готовності з п'ятьма ВК топології «повна сітка» ($\lambda_з$ = 0,05 для $l \geq 1$): *а*) $\mu_в$ = 0,4; *б*) $\mu_в$ = 1,4.

Засоби аналізу захищеності КМ функціонують на мережевому рівні, рівні ОС і рівні додатка.

Найбільшого поширення набули засоби аналізу захищеності мережевих сервісів і протоколів, системного та прикладного програмного забезпечення.

Застосування засобів аналізу захищеності дозволяє оперативно визначити вузли корпоративної мережі, доступні в момент проведення тестування; виявити сервіси та протоколи, які використовуються в мережі, їх налаштування і можливість для несанкціонованої дії (НСД).

Типова схема проведення аналізу захищеності наведена на рис. 6.

Засоби моніторингу захищеності аналізують уразливість мережевих сервісів та протоколів, та системного й прикладного програмного забезпечення.

Враховуючи, що мережеві технології швидко змінюються, статичні захисні механізми (системи розмежування доступу, системи аутентифікації) у багатьох випадках не можуть забезпечити ефективного захисту.

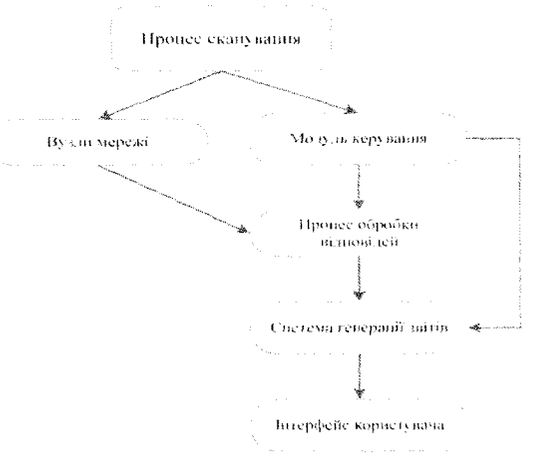


Рис.6. Схема проведення аналізу захищеності КМ.

Виявлення атак – це процес оцінки підозрілих дій, які відбуваються в мережі. Ефективність системи виявлення атак визначається методами моніторингу трафіку.

Статистичний метод. Основними перевагами статистичного підходу є використання апробованого апарату математичної статистики, який описує профіль поведінки суб'єкта.

Для суб'єктів визначаються еталонні профілі. Будь-яке відхилення від еталонного профілю вважається несанкціонованою діяльністю. Статистичні методи є універсальними, однак мають й недоліки:

– «статистичні» системи не чутливі до послідовності виникнення подій;

– граничні значення характеристик, що відстежуються системою виявлення атак базуються, на суб'єктивних оцінках експертів.

Експертні системи. Експертні системи є поширеним засобом виявлення атак. Перевагою такого підходу є практично повна відсутність помилкових тривог.

Структура системи виявлення відхилень включає базу даних (БД) що містить сценарії більшості відомих атак. Для актуалізації експертні системи потребують постійного оновлення БД, перегляду даних в журналах реєстрації.

Основним недоліком систем даного класу є неможливість відстеження нових типів атак.

Інтелектуальні технології на базі нейронних мереж.

Використання нейронних мереж (НМ) є одним із способів подолання вказаних проблем. На відміну від експертних систем НМ проводить аналіз трафіку на відповідність нормальному функціонуванню КМ.

На першому етапі НМ навчають ідентифікації аномальних станів КМ на заздалегідь підібраній вибірці прикладів. Реакція НМ аналізується і система налаштовується таким чином, щоб досягти задовільних результатів. Після початкового періоду навчання НМ забезпечує прийнятний рівень виявлення атак.

Висновки

1. Працездатність мережі цілком залежить від інтенсивності відновлення зв'язності ВК із мережею.

2. Алгоритмом поярусного відбору дозволяє враховувати ймовірності знаходження мережі у всіх станах P_{k_i}, де виконується умова $l \geq l_{mp}$ (т.б. враховується абсолютно всі працездатні стани), тому висока точність оцінки K_{cm} забезпечується повністю.

3. Отримані результати порівняльного аналізу ефективності реконфігурації п'ятирангової топології мережі дозволяють стверджувати, що топологія «повна сітка» є найбільш ефективною для підтримки працездатності та стійкості мережі до виникнення збоїв у ЛЗ.

4. Запропоновано для оцінки *QoS* ввести критерій захищеності КМ як додатковий параметр гарантованої якості обслуговування.

Список літератури

1. Ластовченко М.М., Зубарева Е.А., Саченко В.О. Метод анализа эффективности реконфигурации топологии беспроводных мультисервисных сетей повышенной помехозащищенности // УСиМ. – 2009. – № 6. – С. 79–86.

2. Ластовченко М.М., Русецкий В.Е. Введение критериев интегрального оценивания в системный анализ надежности функционирования широкополосной сети связи // УСиМ. – 2005. – № 2. – С. 86–95.

3. Кучерявый Е.А. Управление трафиком и качество обслуживания в сети Интернет. – Спб.: Наука и Техника, 2004. – 336 с.

4. Жуков И.А., Ластовченко М.М., Искренко Ю.Ю. Анализ процессов адаптивной коррекции радиоспектра при передаче мультимедийного трафика шумоподобными сигналами // Проблеми інформатизації та управління. – 2008. – № 2 (24). – С. 57–64.

5. Безвершенко Е.В., Зубарева Е.А., Шевцова Е.В. Интеллектуальные технологии моделирования процессов передачи мультимедийного трафика // Проблеми інформатизації та управління. – 2008. – № 2 (24). – С. 18–23.