УДК 681.324

Б. Г. Ісмайлов, к. т. н., доц.

АНАЛІЗ РЕЗУЛЬТАТІВ МОДЕЛЮВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ МЕРЕЖАХ ОБСЛУГОВУВАННЯ

У статті проведено порівняльний аналіз результатів математичних та імітаційних методів розв'язання задачі визначення оптимальної програмно-технічної структури систем захисту інформації. Аналіз результатів показує, що вони відрізняються в межах 2 – 10%, а ступінь адекватності аналітичної моделі до досліджуваного об'єкта збільшується зі зменшенням навантаження мережі.

Ключові слова: *система захисту інформації, розподілені мережі обслуговування, моделювання.*

Вступ

Проводиться порівняльний аналіз результатів різних підходів до вирішення проблеми визначення оптимальної програмно-технічної структури систем захисту інформації (СЗІ) [1]. Такі системи створюються між різними розподіленими мережами з одного боку і глобальною мережею – з іншого. Вони інспектують і фільтрують інформацію, що проходить через них. Це свого роду міжмережевий шлюз (gateway), орієнтований на функції інформаційного захисту мереж. Така структура міжмережевих з'єднань дозволяє різко знизити загрозу несанкціонованого доступу в локальну і розподілену мережу за рахунок використання способу маскування (masquerading), коли весь вихідний з РС трафік посилається від імені СЗІ, роблячи РС практично «невидимою». Методи передачі інформації в таких мережах розглядаються в [2 – 4].

Проведений аналіз показує, що перерахування можливих загроз мережі практично нездійсненно через їх велику кількість. Тому на основі деяких характерних особливостей, таких як запрограмовані або незапрограмовані дії, засмічення поштової скриньки, знаходження чорних ходів, захаращення каналу, виведення з ладу комп'ютера і т. д. в [1] пропонується класифікація можливих загроз мережі. Класифікація містить такі загрози як: троянський кінь (ТК), віруси (В), повідомлення, що засмічують поштову скриньку (ПЗПС), чорні ходи (ЧХ), атаки, націлені на відмову сервісу (АНВС), і некоректно працюючі програми (НПП).

Задача визначення характеристик СЗІ в РС вирішується на основі наведеної класифікації можливих загроз мережі. Виходячи з практичних міркувань, можна прийняти, що кількість злочинних програм (повідомлень) складає третину від загального числа повідомлень.

Розподілені мережі, що функціонують в умовах великої інтенсивності при пуассоновському потоці з груповим надходженням, розглянуті в [5]. Інші моделі, пов'язані з розвитком методів маршрутизації і керування потоком, аналізуються в [6]. З метою забезпечення інформаційної безпеки мереж необхідно організувати деяку систему захисту, яка включає сучасні технічні засоби [7] для контролю переданої інформації та їх комплексного захисту від різних впливів. Ці системи містять деякий комплекс програм, який вимагає певного обсягу пам'яті:

– програми, що здійснюють криптографічне шифрування поштових повідомлень, такі як Pretty Good Privacy (PGP);

– утиліти, що дозволяють виявляти і знищувати «шпигунські» програми, наприклад, Ad-aware X cleaner;

– брандмауери, які виявляють і блокують несанкціонований доступ до комп'ютера, не допускають попадання на жорсткий диск «сміття», «шпигунського» програмного забезпечення і «троянів»;

– антивірусні програми (Antivral Toolkit, Kaspresky antivirius, Dr. Web і ін) і різні утиліти, спрямовані на боротьбу з конкретними вірусами.

Проведення періодичного аналізу ефективності СЗІ є однією з основних задач в РС [7]. Шляхом вдосконалення та оптимізації характеристик систем захисту можна забезпечити достатньо високу їх ефективність, яку важко подолати навіть досвідченому зловмисникові. Вирішення вищеописаних проблем вимагає розробки відповідних математичних моделей та методів їх аналізу.

У доступній літературі відомі деякі спроби вирішення зазначених проблем [2 – 4]. Вони в основному використовують методи захисту інформації на рівні імені та пароля користувача, які недостатні для запобігання входу в мережу сторонніх осіб. Крім того, велика кількість потенційних каналів проникнення в мережу ще більше ускладнює захист інформації в мережі. На відміну від зазначених робіт в статті запропоновано альтернативний підхід до вирішення завдання з визначення оптимальної програмно-технічної структури СЗІ. Цей підхід заснований на принципах теорії систем масового обслуговування (СМО), що враховують характеристики впливів можливих загроз на функціонування мережі.

Мета дослідження

Метою цього дослідження є порівняльний аналіз результатів математичних та імітаційних моделей систем захисту інформації в розподілених мережах обслуговування.

Постановка завдання

Проблема полягає в розробці ефективного підходу до вирішення завдання порівняльного аналізу результатів розрахунку та оптимізації функціональної структури системи захисту інформації в РС. В якості математичної моделі СЗІ може слугувати наступна багатоканальна СМО, що складається з N комп'ютерів. Комп'ютери характеризуються переважно інтенсивностями обслуговування, розподіленими за експоненціальним законом, при цьому на вхід системи надходить пуассонівський потік повідомлень з інтенсивністю λ_P, час обслуговування підпорядковується експоненціальному, постійному і ерланговому законам розподілу. Інформація, що надходить, фільтрується і розподіляється по мережі.

Функціонування мережі може бути порушено з боку зловмисників і відновлюється за допомогою комплексу програм як під час передачі повідомлень, так і в проміжку часу, коли передача повідомлень не виконується. Передбачається, що час передачі інформації (T_{ci}), час справної роботи мережі ($T_i = 1/d_i$), час її відбудови (T_{ni}) і час старіння інформації ($T_D = 1/\nu$) в умовах можливих загроз з боку зловмисників розподілені за експоненціальним законом з параметрами μ_i, c_i, d_i, ν відповідно.

Показником ефективності є математичне сподівання ймовірності втрати від несвоєчасного розподілу повідомлень після фільтрації по комп'ютерах мережі, тобто потрібно вирішити наступне завдання [1]:

$$M\left[\bar{P}\right] = \min \sum_{i=1}^{N} p_i q_i \qquad (1)$$

при обмеженнях

$$1 - \sum_{i=1}^{N} p_i = 0, \quad 0 \le P_i \le \mu_i k_i / \lambda, \quad i = \overline{1, N}, \qquad (2)$$

$$\text{де } \mu_i = 1/T_{ci},\ h(p) = 1 - \sum_{i=1}^{N} p_i,\ q_i(p) = p_i,\ q_2(p) = p_i \le \frac{\mu_i k_i}{\lambda}, \qquad (3)$$

$$q_i = \frac{(1 - p_i \lambda h_{1i})}{(1 - p_i \lambda h_{1i} + \nu_i h_{1i}}, \; h_{1i} = \frac{1}{\mu_i k_i}, \; \nu_i = \nu \left[k_i + \frac{(1 - k_i)(\nu - p_i \lambda)}{\nu (1 + \nu T_{ni}} \right], \; i = \overline{1, N} . \qquad (4)$$

Тут прийняті наступні позначення: $\overline{P}$ – імовірність втрати від несвоєчасного розподілу повідомлень по комп'ютерах після фільтрації в РС, p_i – імовірність втрати від непотрапляння повідомлень для передачі на i-ий комп'ютер, q_i – ймовірність втрати в i-му комп'ютері від несвоєчасної доставки повідомлень, k_i – коефіцієнт готовності, T_{ni} – середній час простою.

З метою вирішення задачі (1) – (4) в [1] запропоновано використовувати метод узагальненого приведеного градієнта [8], на основі якого розроблено алгоритми розрахунку і оптимізації характеристик СЗІ за обраним критерієм якості. Цей метод дозволяє дослідити поведінку СЗІ за будь-яких діапазонів зміни структурних і навантажувальних параметрів моделі.

Аналіз результатів математичної моделі СЗІ у РС

Для розрахунку характеристик СЗІ на основі розробленого алгоритму проведені численні обчислювальні експерименти в широких діапазонах зміни як структурних, так і навантажувальних параметрів моделі. Так, для вихідних даних $1/\mu_i = (0{,}042; 0{,}042; 0{,}063)$, $k_i = (0{,}97; 0{,}79; 0{,}81)$, $T_n = (0{,}6; 0{,}9; 1{,}0)$, $\nu = 0{,}5 (T_D = 2)$ досліджено залежності $p_i = f(\lambda), \; i = \overline{1,3}$. Відповідні результати показані на рис. 1.

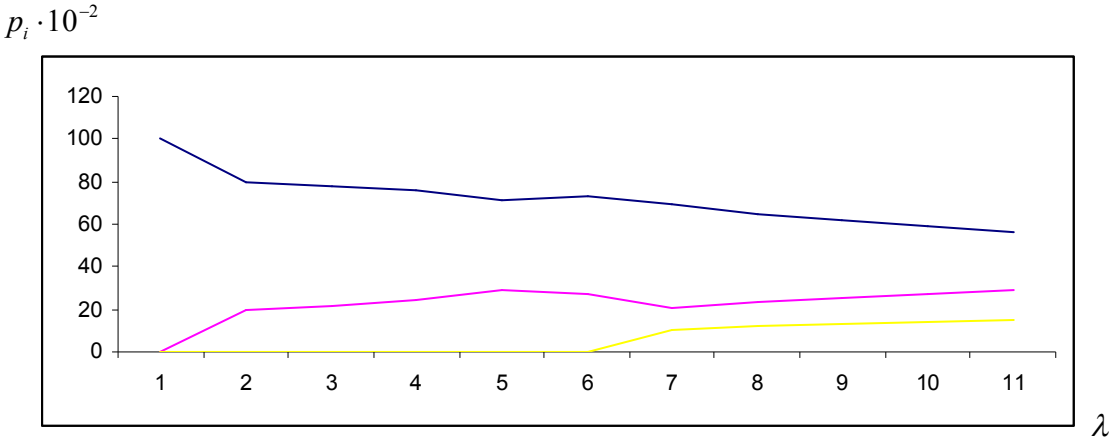
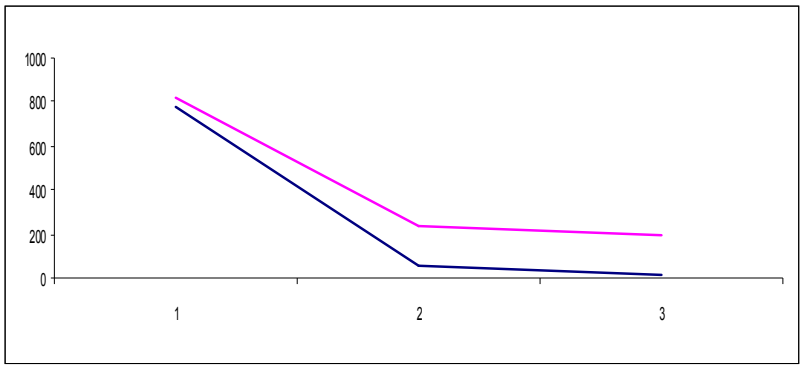


Рис. 1. Залежності $p_i = f(\lambda), \; i = \overline{1,3}$

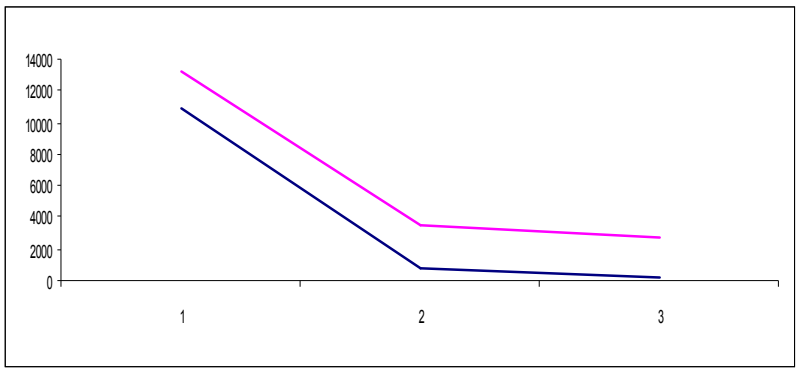
У силу допустимих втрат інформації, показаних на рис. 1, визначено основні характеристики багатоканальної СМО для експоненціального, постійного і ерлангового часу обслуговування. Тут основними характеристиками є L_q – довжина черги, L_s – кількість повідомлень у системі, τ_q – час очікування повідомлень в черзі, τ_s – час перебування повідомлень у системі (рис. 2 – 7, $a = (0{,}95; 0{,}67; 0{,}46)$, L_q, τ_q, – верхня лінія, L_s, τ_s – нижня лінія).

$L_q 10^{-2},\ L_s 10^{-2}$



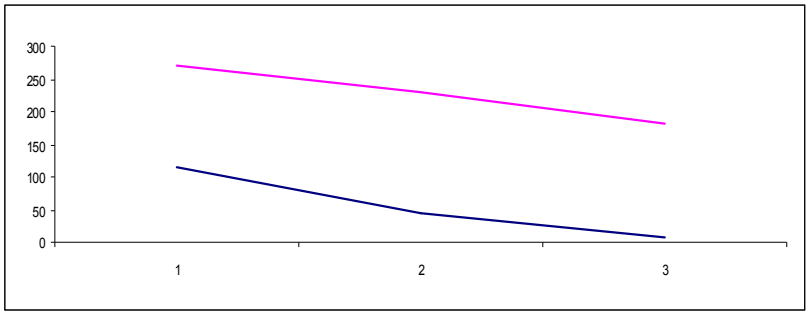
$a = \lambda / \mu N$

Рис. 2. Залежності $L_q = f(a)$, $L_s = f(a)$ для експоненціального часу обслуговування $\tau_q,\ \tau_s$



$a = \lambda / \mu N$

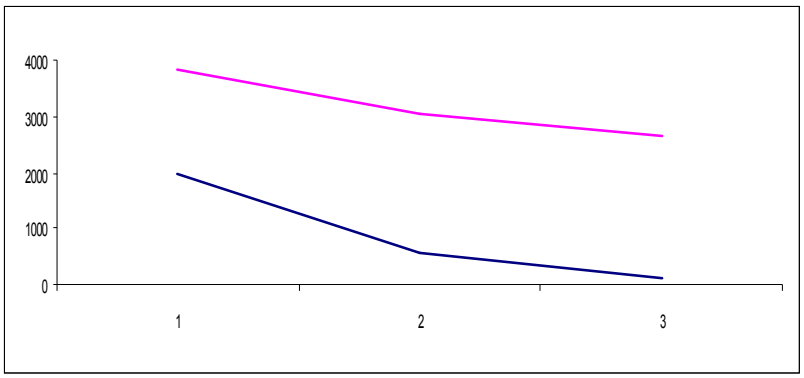
Рис. 3. Залежності $\tau_q = f(a)$, $\tau_s = f(a)$ для експоненціального часу обслуговування $L_q 10^{-2}$, $L_s 10^{-2}$



$a = \lambda / \mu N$

Рис. 4. Залежності $L_q = f(a)$, $L_s = f(a)$ для постійного часу обслуговування

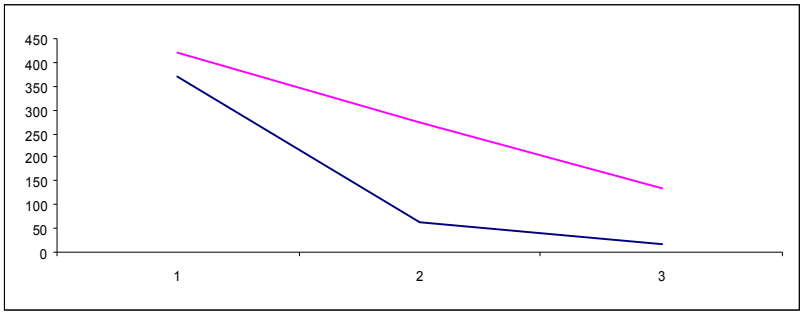
$\tau_q,\ \tau_s$



$a = \lambda / \mu N$

Рис. 5. Залежності $\tau_q = f(a)$, $\tau_s = f(a)$ для постійного часу обслуговування

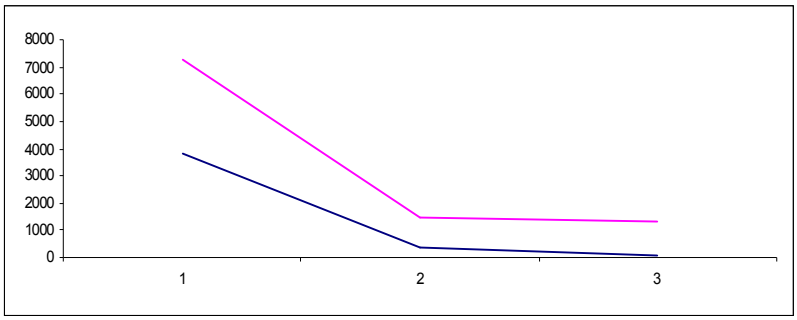
$L_q 10^{-2},\ L_s 10^{-2}$



$a = \lambda / \mu N$

Рис. 6. Залежності $L_q = f(a)$, $L_s = f(a)$ для ерлангового часу обслуговування

$\tau_q,\ \tau_s$



$a = \lambda / \mu N$

Рис 7. Залежності $\tau_q = f(a)$, $\tau_s = f(a)$ для ерлангового часу обслуговування

Отримані результати підтвердили теоретичні очікування щодо поведінки функції втрати від несвоєчасного розподілу повідомлень по комп'ютерах після фільтрації в РС з певною схемою маршруту розподілу повідомлень у мережі в умовах можливих загроз з боку зловмисників.

При побудові СЗІ в РС поряд з аналітичними методами моделювання часто використовують і метод імітаційного моделювання [9]. Останній метод представляє розробникам можливість дослідження об'єктів практично будь-якої складності. При цьому імітаційне моделювання використовують як складову частину системи автоматизації проектування на етапах ескізного і технічного проектування. До числа найбільш широко розповсюджених інструментальних засобів, що забезпечують підтримку прийняття рішення, відноситься General Purpose Simulation System (GPSS) [9].

Аналіз результатів імітаційної моделі СЗІ у РС

Розглядаються варіанти імітаційних моделей СЗІ в РС, які мають наступні схеми маршрутизації повідомлень двох типів. Маршрут обробки повідомлень для першого типу виконується за функціями (операції із захисту інформації) [1 – 3], а для повідомлень другого типу виконується за функціями (операції із захисту інформації) [4 – 6]. Розподілення виконуваних функцій захисту інформації по комп'ютерах k_i, $i = \overline{1,3}$, інтервали часу між повідомленнями, які надходять, і час їх виконання задані.

Потрібно визначити середнє завантаження кожного комп'ютера, середній час обробки повідомлень кожного типу, довжину черг на обробку для комп'ютерів, обсяг пам'яті, необхідний для цього потоку повідомлень. У моделі таймер налаштований на виконання моделювання протягом встановленого модельного часу. При необхідності таймер повинен бути відкоректований. Після прогону моделі імітації СЗІ в РС отримано результати. На основі цих результатів побудовано та досліджено залежності, які показані на рис. 8 – 10.

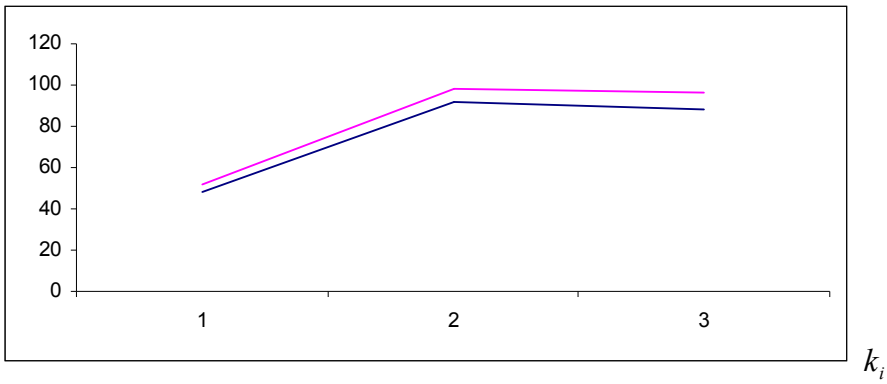


Рис. 8. Середнє завантаження комп'ютерів (у %) k_i, протягом 8 год. (верхня лінія), протягом тижня (нижня лінія)

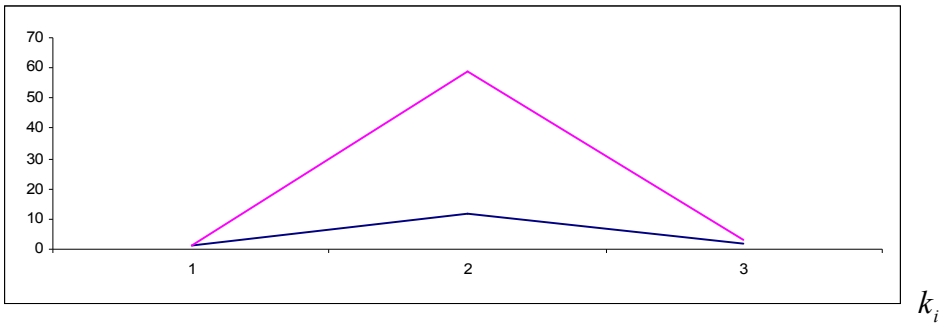


Рис. 9. Максимальна довжина черг до комп'ютерів k_i, протягом 8 год. (верхня лінія), протягом тижня (нижня лінія)

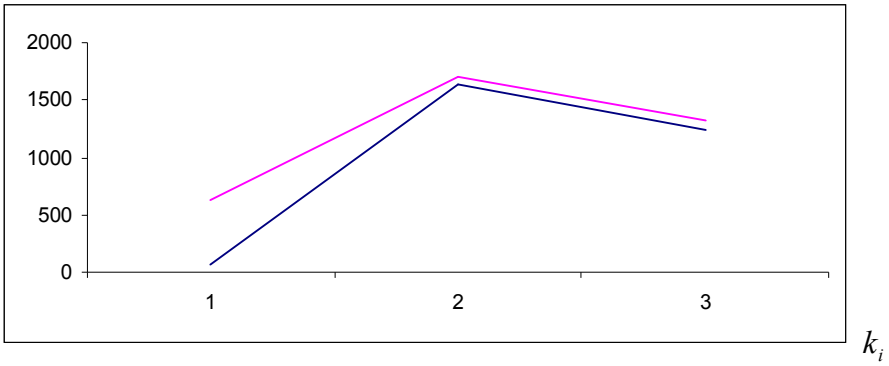


Рис. 10. Середній час обробки повідомлень на комп'ютерах (у хв.) k_i, протягом 8 год. (верхня лінія), протягом тижня (нижня лінія)

За результатами моделювання можна зробити висновок про те, що загальне число оброблених повідомлень протягом 8 годин становить 40, протягом робочого тижня – 142. Ці дані дозволяють розраховувати необхідний обсяг пам'яті для СЗІ в РС. При цьому перший комп'ютер k_1 завантажений на 50% і перевантажений комп'ютер k_2 (про це говорить середній відсоток використання 98% і довжина черги 59 повідомлень). При цьому комп'ютер k_3 завантажений оптимально. Відзначимо, що для підвищення ефективності функціонування СЗІ в РС при цьому потоці повідомлень можна використовувати два комп'ютери.

З метою визначення оптимальної структури СЗІ в РС при заданому потоці повідомлень можна продовжити прогон моделі. Крім того, якщо структуру мережі міняти не можна, то, використовуючи можливості мови моделювання GPSS, можна підібрати такий потік повідомлень, який дозволив би завантажувати мережі оптимально.

Розробка алгоритму аналізу і порівняння результатів математичних та імітаційних методів

З метою порівняльного аналізу результатів математичних та імітаційних методів розроблено алгоритм, який має наступні кроки.

Крок 1. Побудова моделі імітації для різних випадків.

Крок 2. Виконання процесу імітації при нормальних умовах, отримання різних варіантів і обґрунтування моделі.

Крок 3. Порівняння результатів математичних та імітаційних моделей.

Крок 4. Якщо результати математичних та імітаційних моделей збігаються, виконуються імітації для пікового навантаження. В іншому випадку система розширює свої можливості (тобто збільшується значення структурних параметрів).

Крок 5. Здійснюється процес тестування (побудова і обробка РС і перевірка всіх функцій).

Крок 6. Виконання імітації при нормальних умовах і побудови для отримання різних варіантів.

Крок 7. Перевірка збіжності результатів. Якщо вони збігаються, мережа перевіряється додатково в умовах пікових навантажень. В іншому випадку мережа розширює свої можливості і здійснюється перехід до четвертого кроку.

Порівняння результатів математичних та імітаційних моделей здійснюється так:

$$\Delta P = \left[\frac{(P^{\bullet} - P)}{P} \right] \cdot 100\,\%, \qquad (5)$$

де, $P^{\bullet}$, P – значення характеристик математичних та імітаційних моделей відповідно.

На основі розробленого алгоритму аналіз результатів, отриманих після прогону обох моделей, показує, що вони відрізняються в межах 2 – 10%, а ступінь адекватності математичної моделі до досліджуваного об'єкта збільшується зі зменшенням значення навантаження $a = \lambda / \mu N$.

Висновки

Проведено порівняльний аналіз результатів математичних та імітаційних моделей системи захисту інформації в розподілених комп'ютерних мережах. Здійснено обчислювальні експерименти на основі розроблених алгоритмів і отримано чисельні результати. Аналіз результатів обох моделей показує, що вони відрізняються в межах 2 – 10%, а ступінь адекватності математичної моделі до досліджуваного об'єкта збільшується зі зменшенням навантаження.

СПИСОК ЛІТЕРАТУРИ

1. Исмайлов Б. Г. Исследование характеристик систем защиты информации распределенной сети / Б. Г. Исмайлов // Автоматика и вычислительная техника. – Рига: – 2006. – №3. – С. 51 – 59.

2. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М.: ППО «Известия» УДПРФ. – 1997. – 372 с.

3. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. Развитие, итоги, перспективы / В. А. Герасименко // Зарубежная радиоэлектроника. – 1993. – № 3. – С. 3 – 21.

4. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – М.: Издательство Агентства «Яхтсмен». – 1996. – 130 с.

5. Алиев А. А. Анализ характеристик многопотоковых сетей обслуживания / А. А. Алиев, Б. Г. Исмайлов // Радиоэлектроника, информатика и управление. – Запорожье: 2001. – № 2. с. 66 – 69.

6. Maxchemchuk N. F. Routing and flow control in high–speed wide area networks / N. F. Maxchemchuk, M. Ei. Zarki // Proc. of the IEEE. – 1990. – Vol. 78. – N1. – P. 204 – 221.

7. Алябев С. В. Проблемы защиты информации в сети промышленного предприятия / С. В. Алябев // Сб. трудов ПУКИ. – 2003. – Выпуск 8. Воронеж: Центральное Черноземное книжное издательство. – С. 69 – 70.

8. Химмелблау Д. Прикладное нелинейное программирование / Д. Химмелблау. – М.: Мир, 1975. – 540 с.

9. Шрайбер Т. Дж. Моделирование на GPSS / Т. Дж. Шрайбер – М.: Машиностроение, 1980. – 592 с.

Ісмайлов Балами Гасимов огли – доцент кафедри інформатики. Email: Balemi@rambler.ru
Сумгаїтський державний університет.