$f_{1,j_0}(t)\equiv 0$ зовні Δs, $f_{2i}(t)\equiv 0$ при $i\neq i_0$, $f_{2,i_0}(t)\neq 0$ в Δs, $f_{2,i_0}(t)\equiv 0$ зовні Δs. Для цього вибору рівняння (33) буде еквівалентним до

$$\int\limits_{t_0-\Delta t}^{t_0+\Delta t}\int\limits_{x_0-\Delta x}^{x_0+\Delta x} f_{2,i_0}(x)\left[\overline{h_{j_0,i_0}(t,x,\lambda)}-g_{i_0,j_0}(x,t,\lambda)\right]f_{1,j_0}(t)dxdt=0,$$

і, оскільки $f_{2,i_0}(x)f_{1,j_0}(t)\neq 0$ в Δs, очевидно, вираз у квадратних дужках перетворюється в нуль десь у цій області. Нехай Δx і Δt прямують до нуля. Тоді в границі ми матимемо $\overline{h_{j_0,i_0}(t_0,x_0,\lambda)}=g_{i_0,j_0}(x_0,t_0,\lambda)$ і внаслідок довільності вибору векторів $\mathbf{f}_1(t)$, $\mathbf{f}_2(x)$ та точок x_0, t_0 ($x_0\neq t_0$) отримаємо твердження теореми.

Отримані результати дозволяють вивчати й інші задачі, зокрема задачі на розвинення за власними функціями. Аналогічні результати можна отримати й у випадку векторного сингулярного квазідиференціального оператора.

1. Наймарк М.А. Линейные дифференциальные операторы. – М.: Наука, 1969. – 528 с.
2. Кац И.С., Крейн М.Г. О спектральных функциях струны // Дискретные и непрерывные граничные задачи / Ф.Аткинсон. – М.: Мир, 1968. – С.648–731.
3. Альбеверио С., Гестези Ф., Хёэг-Крон Р., Хольден Х. Решаемые модели в квантовой механике: Пер. с англ. – М.: Мир, 1991. – 566 с.
4. Махней О.В. Асимптотика власних значень і власних функцій сингулярного диференціального оператора на скінченному інтервалі // Мат. методи та фіз.-мех. поля. – 2001. – Т.44, №2. – С.17–25.
5. Махней О.В. Функція Гріна сингулярного диференціального оператора та її властивості // Матем. студії. – 2002. – Т.18, №2. – С.147–156.
6. Махней О.В. Сингулярні квазідиференціальні оператори на скінченному інтервалі: Автореф. дис. ... канд. фіз.-мат. наук: 01.01.02 / Одеський нац. ун-т ім. І.І.Мечникова. – Одеса, 2005. – 16 с.
7. Шин Д. О квази дифференциальных операторах в гильбертовом пространстве // ДАН СССР. – 1938. – Т.18, №8. – С.523–526.
8. Шин Д. О решениях линейного квазидифференциального уравнения n-го порядка // Матем. сборник. – 1940. – Т.7 (49), №3. – С.479–527.
9. Халанай А., Векслер Д. Качественная теория импульсных систем: Пер. с рум. – М.: Мир, 1971. – 312 с.
10. Стасюк М.Ф., Таций Р.М. Корректные дифференциальные системы с мерами // Вестн. Львов. политехн. ин-та: Дифференц. уравн. и их приложения. – 1988. – №222. – С.89–90.
11. Тацій Р.М. Дискретно-неперервні крайові задачі для диференціальних рівнянь з мірами: Автореф. дис... д-ра фіз.-мат. наук: 01.01.02 / Львів. держ. ун-т ім. І.Франка. – Львів, 1994. – 37 с.

In this work a Green matrix-function of boundary problem for vector differential equation with generalized functions in coefficients is constructed. With the help of obtained expressions for adjoint boundary conditions the property about the relationship between Green functions of adjoint boundary problems is proved.

Key words: *Green function, vector differential equation, quasiderivatives, generalized functions.*

УДК 004.942+004.056.57
ББК 22.181

Л.С. Возняк, Н.О. Возняк

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ПОШИРЕННЯ КОМП'ЮТЕРНИХ ВІРУСІВ В ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ

Розглянуто математичні моделі поширення цифрових інфекцій в інформаційних системах. На основі наявних у глобальній мережі Інтернет статистичних даних перевірено відповідність побудованих математичних моделей для різних типів комп'ютерних вірусів. Побудована математична модель поширення комп'ютерного вірусу в інтермережі, яка складається з К-підмереж. Здійснено чисельний розв'язок запропонованої моделі.

Ключові слова: *математичне моделювання, комп'ютерні віруси, комп'ютерні епідемії.*

Математичний аналіз моделей поширення комп'ютерних вірусів в обчислювальних мережах, що описуються звичайними диференціальними рівняннями

SIS модель поширення комп'ютерного вірусу. Перша класична модель поширення вірусу віспи, запропонована ще в 1760 році Даніелем Бернуллі, передбачає поділ популяції на хворих особин і тих, хто потенційно може заразитися. У термінах комп'ютерних мереж будемо розглядати заражені хости (host) і хости, що можуть бути зараженими. Можемо записати найпростішу математичну модель поширення вірусу:

$$\frac{dJ(t)}{dt} = \beta J(t)\left[N - J(t)\right], \tag{1}$$

де $J(t)$ – кількість заражених хостів у момент часу t, N – загальна кількість хостів, β – коефіцієнт зараження. Привівши цю модель до безрозмірного вигляду, ввівши заміни

$$a(t) = \frac{J(t)}{N}, \quad k = \beta N,$$

одержимо таке рівняння:

$$\frac{da(t)}{dt} = ka(t)\left[1 - a(t)\right]. \tag{2}$$

Останнє рівняння можна модифікувати, ввівши в нього доданок, який у біологічних системах характеризує смертність:

$$\frac{da(t)}{dt} = ka(t)\left[1 - a(t)\right] - da(t), \tag{3}$$

тут d – коефіцієнт виходу інфікованих хостів із ладу.

Для такої системи існує точний розв'язок:

$$a(t) = \frac{a_0(1-\rho)}{a_0 + (1 - \rho - a_0)e^{-(k-d)t}}, \quad \rho = \frac{k}{d}, \; a_0 = a(t_0). \tag{4}$$

Аналіз розв'язку показує, що при $\beta < d$ частка заражених хостів поступово прямує до нуля. Якщо $\beta > d$, то для малих значень t функція зростає експоненційно до того моменту, поки більшість хостів виявиться зараженими. При $t \to \infty$ змінюється характер зростання і функція досягає свого екстремуму $1 - \rho$, коли всі хости виявилися зараженими.

SIR модель поширення комп'ютерного вірусу. Для моделювання поширення біологічних вірусів, а також для поширення вірусів комп'ютерних зручно скористатися відомою SIR моделлю [3]. У випадку поширення комп'ютерних вірусів вона базується на поділі хостів із мережі на три підгрупи: незахищені (susceptible), інфіковані (infectious), імунізовані (removed). Нехай $S(t)$ – кількість незахищених хостів у момент часу t, $I(t)$ – кількість заражених хостів у момент часу t, $R(t)$ – кількість захищених хостів у момент часу t. SIR модель описується системою звичайних диференційних рівнянь:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\beta S(t)I(t), \\ \dfrac{dI(t)}{dt} = \beta S(t)I(t) - \mu I(t), \\ \dfrac{dR(t)}{dt} = \mu I(t), \end{cases} \tag{5}$$

де $\beta > 0$ – коефіцієнт зараження незахищених хостів, $\mu > 0$ – коефіцієнт імунізації.

Для того, щоб одержати задачу Коші, систему рівнянь (5) доповнюють початковими умовами виду:

$$S(t_0) = S_0, I(t_0) = I_0, R(t_0) = R_0, t \ge t_0. \tag{6}$$

Одне з базових припущень, яке використовується при побудові моделі (1) – (2), полягає в тому, що хост одержує імунітет проти вірусного зараження лише тоді, коли він буде зараженим, проте не виключено, що деякі хости будуть імунізовані ще до того, коли на них потрапить вірус. Серед інших факторів, які не враховано в моделі (5), – це виокремлення в динаміці розвитку вірусу моментів, коли ще відсутній ефективний антивірусний захист (вірус може вільно розповсюджуватися в мережі) і коли такий антивірус створено (тоді розвиток вірусу проходить згідно із SIR моделлю).

PSIDR модель поширення комп'ютерного вірусу. Запропонована в [4] модель поширення хробака є уточненням SIR моделі. Вона складається з чотирьох (а не з трьох, як у класичній моделі) станів: "незахищений", "інфікований", "ідентифікований", "імунізований". Укажемо на основні особливості цієї моделі:

- Безпосередня імунізація. Часто на хости завчасно встановлюється відповідне антивірусне програмне забезпечення, яке оберігає комп'ютер від інфікування (за умови, що вакцина проти цього вірусу вже існує). Тоді частина комп'ютерів переходить зі стану "незахищені" в стан "захищені", обминаючи, таким чином, стани "інфікований" та "ідентифікований".
- Наявність антивірусу. Для того, щоб хости можна було вилікувати, необхідно, щоб був розроблений антивірус. Часто між появою вірусу й розробкою такого антивірусу минає певний час. Тоді перебіг комп'ютерної епідемії можна розмежувати на два етапи:

- *доідентифікаційний:* у цей час хробак вільно поширюється по мережі, оскільки користувачі ще не виявили його присутності. Хости з певною ймовірністю вражаються вірусом, лікування ще не відбувається;

- *післяідентифікаційний:* вірус ідентифіковано й активізуються заходи щодо боротьби з ним. Ще неінфіковані хости імунізуються, а вже хворі – лікуються.

- Лікування. Після ідентифікації інфікованого хоста минає певний час (особливо це стосується великих підприємств), поки цей вірус буде знищено, а комп'ютер імунізовано. Тому в даній моделі введено проміжний стан.

Отже, введемо в розгляд параметр π, який характеризує час, необхідний для ідентифікації вірусу. Крім того, виділимо ще один стан, який характеризує хости, на яких вірус уже ідентифіковано, але вони ще вважаються зараженими.

Одержимо так звану PSIDR (progressive susceptible-infected-identified-remote) модель:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\beta S(t)I(t), \\ \dfrac{dI(t)}{dt} = \beta S(t)I(t), \quad t \le \pi, \\ N = S(t) + I(t), \end{cases} \tag{7}$$

$$\begin{cases} \dfrac{dS(t)}{dt} = -\beta S(t)I(t) - \mu S(t), \\ \dfrac{dI(t)}{dt} = \beta S(t)I(t) - \mu I(t), \\ \dfrac{dD(t)}{dt} = \mu I(t) - \delta D(t), \qquad t > \pi. \\ \dfrac{dR(t)}{dt} = \delta D(t) + \mu S(t), \\ N = S(t) + I(t) + D(t) + R(t), \\ S(0) > 0, I(0) > 0, D(0) = 0, R(0) = 0, \end{cases} \tag{8}$$

Тут $S(t), I(t), D(t), R(t)$ – відповідно кількість незахищених, інфікованих хостів, на яких ідентифіковано інфекцію, та імунізованих хостів, β – коефіцієнт поширення інфекції, δ – час між ідентифікацією та імунізацією хоста, μ – коефіцієнт імунізації хостів. Аналіз моделі в залежності від значень параметрів $(\beta, \mu, \delta, \pi)$ і порівняльний аналіз із класичною моделлю Кермака-Мак Кендріка можна знайти в [3].

Математична модель поширення комп'ютерного вірусу в інтермережі

Розглянемо складну комп'ютерну мережу (Інтернет) як сукупність пов'язаних мереж. Мережі, що входять у складну мережу, назвемо підмережами.

Для узагальнення моделі (5) на випадок взаємопов'язаних K-підмереж ми ввели коефіцієнти проникнення між підмережами δ_{ij}, які характеризують якість антивірусного бар'єру між підмережами, й отримали таку модель:

$$\begin{cases} \dfrac{dS_i(t)}{dt} = -\beta_i S_i(t) I_i(t) - \sum\limits_{\substack{j=1\\ j\neq i}}^{K} \delta_{ji} S_i(t) I_j(t), \\ \dfrac{dI_i(t)}{dt} = \beta_i S_i(t) I_i(t) - \mu_i I_i(t) + \sum\limits_{\substack{j=1\\ j\neq i}}^{K} \delta_{ji} S_i(t) I_j(t), \quad i = 1,2,\ldots,K, \\ \dfrac{dR_i(t)}{dt} = \mu_i I_i(t), \\ N_i = S_i(t) + I_i(t) + R_i(t), \end{cases} \tag{9}$$

де S_i – кількість незахищених хостів в i-ій підмережі, I_i – кількість інфікованих хостів в i-ій підмережі, R_i – кількість захищених хостів в i-ій підмережі, β_i – швидкість поширення вірусу в i-ій підмережі, μ_i – швидкість імунізації хостів в i-ій підмережі відповідно. Модель (9) доповнюється початковими умовами:

$$\begin{cases} S_i(t_0) = S_{i0}, \\ I_i(t_0) = I_{i0}, \quad i = 1,2,\ldots,K. \\ R_i(t_0) = R_{i0}. \end{cases} \tag{10}$$

Кожен із коефіцієнтів δ_{ij} задає ймовірності попадання вірусу з підмережі i в підмережу j.

Аналіз поширення комп'ютерного вірусу в інтермережі. Визначимо для моделі (9) умови, за яких можливий розвиток епідемії в підмережі. Умовою початку епідемій в підмережах є додатне значення похідної від функції кількості інфікованих хостів у підмережі по часу:

$$\left.\frac{dI_i}{dt}\right|_{t=t_0} = \beta_i S_{i0} I_{i0} - \mu_i I_{i0} + \sum_{\substack{j=1\\ i\neq j}}^{K} \delta_{ij} S_{i0} I_{j0} = S_{i0}\left(\beta_i I_{i0} + \sum_{\substack{j=1\\ i\neq j}}^{K} \delta_{ij} I_{j0}\right) - \mu_i I_{i0} > 0, \tag{11}$$

звідки

$$S_{i0} > \frac{\mu_i I_{i0}}{\beta_i I_{i0} + \sum\limits_{\substack{j=1\\ i\neq j}}^{K} \delta_{ij} I_{j0}}. \tag{12}$$

Одержаний результат означає, що в підмережі i не почнеться епідемія комп'ютерного вірусу, якщо початкова кількість незахищених хостів не перевищує певної величини.

Спробуємо оцінити вплив коефіцієнтів проникності δ_{ij} на нерівність (12). Для спрощення викладок вважаємо, що кількість інфікованих хостів у кожній підмережі в початковий момент часу є однаковою. Розглянемо таку функцію:

$$S_{i0}(\delta_{i1},\ldots,\delta_{iK}) = \frac{\mu_i}{\beta_i + \sum\limits_{\substack{j=1\\ i\neq j}}^{K} \delta_{ij}}. \tag{13}$$

Оскільки ми розглядаємо коефіцієнти проникнення вірусу як імовірності попадання вірусу з підмережі в підмережу, то $0 \le \delta_{ij} \le 1$. Максимальне значення

$$S_{i0}^{\max} = \frac{\mu_i}{\beta_i}$$

функції (13) досягається в точці (0,...,0), а мінімальне –

$$S_{i0}^{\min} = \frac{\mu_i}{\beta_i + K}$$

в точці $(1,\ldots,1)$.

Таким чином, можна зробити висновок, що зі зростанням значень коефіцієнтів проникнення між підмережами зменшується порогове значення, при якому починається епідемія. А отже, чим більшими є коефіцієнти проникнення між підмережами, тим швидше розпочнеться епідемія в іншій підмережі.

З нерівності (11) можемо одержати ще одну оцінку початку розвитку епідемії:

$$I_{i0} > \frac{S_{i0}\sum_{\substack{j=1 \\ i\neq j}}^{K}\delta_{ij}I_{j0}}{\beta_i S_{i0} - \mu_i} \tag{14}$$

Останній результат означає, що в підмережі i не почнеться епідемія комп'ютерного вірусу доти, доки початкова кількість хворих хостів у підмережі i не задовольняє нерівності (14).

Епідеміологічний поріг. При математичному дослідженні кожної епідеміологічної моделі важливо визначити її епідеміологічний поріг. Ця величина вказує на те, за якої умови можливе поширення хвороби при малій кількості початково інфікованих хостів.

Для обчислення значення епідеміологічного порога потрібно дослідити стійкість системи звичайних диференційних рівнянь (9) у її стаціонарній точці, де відсутні інфіковані хости:

$$\left(S_i = S^0, I_i = 0, R_i = 0\right) \text{ для } i = 1,2. \tag{15}$$

Дослідити стійкість системи (9) в стаціонарній точці (15) можна або записавши відповідну функцію Ляпунова, або визначивши власні значення матриці Якобі, обчисленої в стаціонарній точці (15).

Матриця Якобі для моделі (9) має вигляд:

$$J = \begin{pmatrix} -\beta_1 I_1 - \delta_{BA} I_2 & -\beta_1 S_1 & 0 & 0 & -\delta_{BA} S_1 & 0 \\ \beta_1 I_1 + \delta_{BA} I_2 & \beta_1 S_1 - \mu_1 & 0 & 0 & \delta_{BA} S_1 & 0 \\ 0 & \mu_1 & 0 & 0 & 0 & 0 \\ 0 & -\delta_{AB} S_2 & 0 & -\beta_2 I_2 - \delta_{AB} I_1 & -\beta_2 S_2 & 0 \\ 0 & \delta_{AB} S_2 & 0 & \beta_2 I_2 + \delta_{AB} I_1 & \beta_2 S_2 - \mu_2 & 0 \\ 0 & 0 & 0 & 0 & \mu_2 & 0 \end{pmatrix} \tag{16}$$

В околі стаціонарної точки $(S_i = S_i^0, I_i = 0, R_i = 0), i = 1,2$ матриця Якобі має вигляд:

$$J_h = \begin{pmatrix} 0 & -\beta_1 S_1^0 & 0 & 0 & -\delta_{BA} S_1^0 & 0 \\ 0 & \beta_1 S_1^0 - \mu_1 & 0 & 0 & \delta_{BA} S_1^0 & 0 \\ 0 & \mu_1 & 0 & 0 & 0 & 0 \\ 0 & -\delta_{AB} S_2^0 & 0 & 0 & -\beta_2 S_2^0 & 0 \\ 0 & \delta_{AB} S_2^0 & 0 & 0 & \beta_2 S_2^0 - \mu_2 & 0 \\ 0 & 0 & 0 & 0 & \mu_2 & 0 \end{pmatrix} \tag{17}$$

Обчисливши власне значення матриці (17) з найбільшою дійсною частиною

$$\operatorname{Re}\lambda_{\max} = \frac{1}{2}\left(a_1 + a_2 + \sqrt{(a_1 - a_2)^2 + 4a_3 a_4}\right), \tag{18}$$

де

$$a_1 = \beta_1 S_1^0 - \mu_1,\; a_2 = \beta_2 S_2^0 - \mu_2,\; a_3 = \delta_{BA} S_1^0,\; a_3 = \delta_{AB} S_2^0, \tag{19}$$

ми визначимо умову епідеміологічного порога, оскільки стійкість матриці (17) визначається умовою $\operatorname{Re}\lambda_{\max} < 0$:

$$a_1 + a_2 + \sqrt{(a_1 - a_2)^2 + 4a_3 a_4} < 0. \tag{20}$$

Остання умова й визначає епідеміологічний поріг.

Базовий репродуктивний коефіцієнт. Епідеміологічний поріг дозволяє визначити так званий базовий репродуктивний коефіцієнт R_0 (кількість захворювань, до яких призведе один інфікований хост в цілком незахищеній мережі). Ми можемо визначити його з умови (8) роботи [4]:

$$R_0 = \frac{\beta_1 S_1^0 + \beta_2 S_2^0 + \sqrt{\left(\beta_1 S_1^0 - \mu_1 - \beta_2 S_2^0 + \mu_2\right)^2 + 4\delta_{AB}\delta_{BA}S_1^0 S_2^0}}{\mu_1 + \mu_2}. \tag{21}$$

Якщо базовий репродуктивний коефіцієнт $R_0 < 1$, то епідемія не розпочнеться. Інакше при наборі параметрів моделі, що задовольняють умову $R_0 > 1$, існує тенденція до збільшення кількості інфікованих хостів.

Аналіз епідеміологічного порога. Аналізуючи нерівність (20), бачимо, якщо одна з підмереж є "непропускною" для вірусів із другої підмережі $\delta_{AB} = 0 \vee \delta_{BA} = 0$, то зміна коефіцієнта проникності вірусу для іншої підмережі ніяк не впливає на величину епідеміологічного порога. Цей результат є дещо несподіваним, оскільки ми очікували, що коефіцієнти проникнення вірусу між підмережами повинні мати незалежний вплив на порогове значення. Одержаний результат пояснюємо тим, що в околі стаціонарної точки, в якій відсутні інфіковані хости, малі збурення хвороби не мають впливу на поширення вірусу в інші підмережі.

Інший важливий результат одержимо, поклавши $\beta = \beta_1 = \beta_2$, $\mu = \mu_1 = \mu_2$, $\delta_{AB} = \delta_{BA}$, $S_0 = S_1^0 = S_2^0$ (тобто підмережі зв'язані між собою і містять однакову кількість хостів, а коефіцієнти поширення вірусу, імунізації хостів і проникнення вірусу між підмережами збігаються), тоді умову епідеміологічного порога (20) можна переписати:

$$\frac{\beta_0 S_0 + \delta S_0}{\mu} < 1 \Rightarrow S_0 < \frac{\mu}{\beta + \delta}. \tag{22}$$

Зауважимо, що для $\delta = 0$ одержимо $S_0 < \dfrac{\mu}{\beta}$ – відому умову епідеміологічного порога для класичної SIR моделі.

З нерівності (22) випливає, що чим більшим є коефіцієнт проникності вірусу між підмережами, тим меншим є епідеміологічний поріг системи загалом.

Числові дослідження поширення вірусу для двох підмереж. Розглянемо складну мережу, яка складається з трьох підмереж. Кожна підмережа містить 1000 хостів. У початковий момент часу всі хости є незахищеними, а один у третій підмережі є інфікованим. У цьому випадку початкові умови задачі коші є такими:

$$S_{10} = 1000, I_{10} = 0, R_{10} = 0, S_{20} = 1000, I_{20} = 0, R_{20} = 0,$$
$$S_{30} = 999, I_{30} = 1, R_{30} = 0\,.$$

Вхідні параметри $\beta_i, \mu_i, i = \{1,2,3\}$, які характеризують швидкості поширення вірусу і швидкості імунізації хостів для кожної з підмереж, виберемо як такі, що характеризують поширення хробака CodeRed у мережі Internet [5]: $\beta_i = 0.8 \cdot 10^{-5}, \mu_i = 0.01, i = \{1,2,3\}$. Поширенню цього хробака присвячено декілька досліджень [4; 5], тому ми можемо порівняти одержані результати з результатами, одержаними в інших роботах.

Зокрема, для випадку, коли підмережі не пов'язані між собою, тобто значення всіх коефіцієнтів проникності рівне нулю, одержано такий результат: у першій та другій підмережах ніяких змін не відбувається, кількість незахищених комп'ютерів є сталою і рівною 1000, а кількість імунізованих та інфікованих є рівною нулю.

Розглянемо випадок, коли підмережі пов'язані між собою з коефіцієнтами $\delta_A = \delta_{12} = \delta_{21} = 0$, $\delta_B = \delta_{23} = \delta_{32} = 10^{-3}$, $\delta_C = \delta_{13} = \delta_{31} = 10^{-6}$, що відповідає ситуації, коли підмережі 1 і 2 не зв'язані, підмережі 2 і 3 зв'язані з коефіцієнтом проникнення 10^{-3}, підмережі 1 і 3 зв'язані з коефіцієнтом проникнення 10^{-6}. Виявляється, що в першій та другій початково незаражених підмережах інфікування проходить із деяким запізненням.

Випадок, коли підмережі пов'язані між собою з коефіцієнтами проникності $\delta_A = \delta_{12} = \delta_{21} = \delta_B = \delta_{23} = \delta_{32} = \delta_C = \delta_{13} = \delta_{31} = 10^{-6}$, відповідає ситуації, коли всі підмережі є зв'язаними з однаковими коефіцієнтами проникнення 10^{-6}. У цьому випадку в першій та другій початково незаражених підмережах інфікування так само проходить із деяким запізненням, як і в попередньому випадку, але запізнення є сталим.

Нами проводилося дослідження впливу значення коефіцієнта проникнення між підмережами на поширення вірусу. Результат було одержано для моделі (9) у випадку двох підмереж, зв'язаних із коефіцієнтами $\delta = \{10^{-1}, 10^{-2}, 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}\}$ для тих самих початкових умов, що й у попередній задачі. Розглядалися розв'язки $I(t)$ моделі (9) при різних значеннях параметрів δ (для спрощення вважатимемо, що в кожному окремо взятому випадку взаємовплив підмереж є однаковим). Одержаний розв'язок дозволяє стверджувати, що зі зменшенням зв'язності мережі збільшується час відставання між розвитком епідемії. У той же час спостерігаємо, що зменшення зв'язності мережі майже не призводить до зменшення кількості уражених хостів.

Таким чином, проведені дослідження динаміки поширення вірусів в інтермережах показали, що значну роль у швидкості поширення комп'ютерних вірусів відіграє активність обміну інформацією між мережами та наявність антивірусного бар'єру в точках взаємопід'єднання мереж. При побудові сучасних комп'ютерних мереж необхідно враховувати величину епідеміологічного порога, оскільки таким чином можна суттєво знизити ймовірність масового враження хостів у підмережі. Розробляючи стратегію захисту інтермережі, варто брати до уваги не лише захищеність окремо взятих підмереж, а й вплив взаємозв'язків між ними на стійкість до вірусу системи загалом.

1. Moore D., Shannon C., Voelker G.M., Savage S. Internet Quarantine: Requirements for Containing Self-Propagating Code / San Diego Supercomputer Center, University of California. – San Diego: INFOCOM, 2003.
2. Pande R. Using Plant Epidemiological Methods To Track Computer Network Worms.
3. Kermack W.O., McKendrick A.G. A contribution to the mathematical theory of epidemics // Proceedings of the Royal Society of London Series A. – 1927. – P.55–83.
4. Leveille J. Epidemic Spreading in Technological Networks. – 2002 / HP, Technical Report: HPL-2002-287.
5. Zou C.C., Gong W., Towsley D. Code Red Worm Propagation Modeling and Analysis // Conference on Computer and Communications Security archive Proceedings of the 9th ACM conference on Computer and communications security. – Washington: DC, 2002. – P. 138–147.
6. Возняк Н.О., Щербатий М.В. Поширення вірусів в інформаційних системах // Сучасні проблеми прикладної математики та інформатики: Тези доп. Десятої Всеукраїнської наукової конференції (Львів, 23–25 вересня 2003 р.). – Львів, 2003. – С. 37.

Mathematical models of digital infections spreading in informational systems has been overviewed. Based on statistical data given from Internet it has been investigated correctness of prepared mathematical models. It has been built the model of computer virus spreading in the internetwork which consists of K networks. Numerical solution has been also provided.

Key words: *mathematic modelling, computer viruses, computer epidemic.*