

УДК 519.622.2

Варех Н. В., Вольфсон О. Я., Падалка О. А.

Дніпропетровський національний університет імені Олеся Гончара

**ДОСЛІДЖЕННЯ ДИНАМІКИ РОЗПОВСЮДЖЕННЯ
КОМП'ЮТЕРНОГО ВІРУСУ В МЕРЕЖІ**

Досліджено динаміку життєвого циклу комп'ютерного вірусу, яка описується системами з післядією.

Ключові слова: *SIR; інкубаційний період; антивірус; запізнювання; метод кроків.*

Исследована динамика жизненного цикла компьютерного вируса, которая описывается системами с последствием.

Ключевые слова: *SIR; инкубационный период; антивирус; запаздывание; метод шагов.*

The dynamics of the life cycle of a computer virus is investigated in this work. Virus life cycle is described with delayed differential equations systems.

Keywords: *SIR; incubation period; antivirus; delay; step's method.*

Вступ. У наш час глобальною стала проблема зараження комп'ютерів хакерськими, фішинговими програмами та вірусами. Вберегтися від цього складно навіть професійному користувачу ПК, навіть із найсучаснішим антивірусом. Наприклад, лише у цьому році з'явилося два глобальних комп'ютерних віруси WannaCry та Xdata. У зв'язку з цим дослідження динаміки розповсюдження комп'ютерних вірусів у мережі є дуже корисним та актуальним.

Аналіз літературних даних. Широкою популярністю в математичному моделюванні епідемій користується робота [1]. Ця модель вважається узагальненою, оскільки підхід до моделювання, який запропонували автори, використовується і сьогодні.

Однак з'явилися більш сучасні роботи, які також описують процес моделювання хвороб та епідемій, причому в систему диференціальних рівнянь вводиться відхилення аргументу. Наприклад, [2], яка була опублікована у 2001 році. А також робота [3], яка була опублікована у 2013 році.

Постановка задачі. В основу дослідження було взято SIR-модель Kermack and McKendrick [1], в якій популяція індивідів (у нашому випадку – мережа комп'ютерів) розділена на декілька груп:

1) *група сприятливих індивідів*: $S(t)$ – чутливі індивіди, в певний момент часу можуть захворіти;

2) *група інфікованих індивідів*: $I(t)$ – заражені, вони здатні передавати інфекцію сприятливим до неї індивідам;

3) *група резистентних індивідів*: $R(t)$ – це можуть бути індивіди, які перехворіли та набули імунітету до хвороби або індивіди, несприятливі до інфекції. Вони не здатні передавати хворобу іншим та хворіти знову.

В роботі поставлено за мету дослідити існуючу модель та на її основі побудувати нову модель з парною та непарною кількістю диференціальних рівнянь із відхиленням у кожному рівнянні.

Основний матеріал. Базова модель без урахування резистентної групи індивідів та без відхилення аргументу має вигляд:

$$\begin{cases} \frac{dS}{dt} = \mu N - \frac{\beta SI}{N} - \mu S + \gamma I, \\ \frac{dI}{dt} = \frac{\beta SI}{N} - \gamma I - \mu I, \end{cases}$$

де β – частота зараження, $\frac{1}{\gamma}$ – середня тривалість інфекційного

періоду, μ – коефіцієнт виживання.

Було розроблено програму, яка будує графіки, що відображають життєвий цикл вірусу по групах комп'ютерів, де можна побачити початкові кількості комп'ютерів у групах та як вони змінюються із часом під впливом вірусу.

На рис. 1 видно як змінюються чисельності сприйнятливих до вірусу комп'ютерів та комп'ютерів, заражених вірусом.

На основі цієї моделі було побудовано і досліджено моделі з післядією, стан яких визначається не тільки теперішнім часом, а й минулим.

Розглянемо модель із «інкубаційним періодом» на двох групах індивідів, яка описується такою системою з двох диференціальних рівнянь:

$$\begin{cases} \frac{dS}{dt} = \mu N - \frac{\beta SI(t - \tau(t))}{N} - \mu S + \gamma I(t - \tau(t)), \\ \frac{dI}{dt} = \frac{\beta SI(t - \tau(t))}{N} - \gamma I(t - \tau(t)) - \mu I(t - \tau(t)), \end{cases}$$

де β – частота зараження, $\frac{1}{\gamma}$ – середня тривалість інфекційного

періоду, μ – коефіцієнт виживання/смертності.

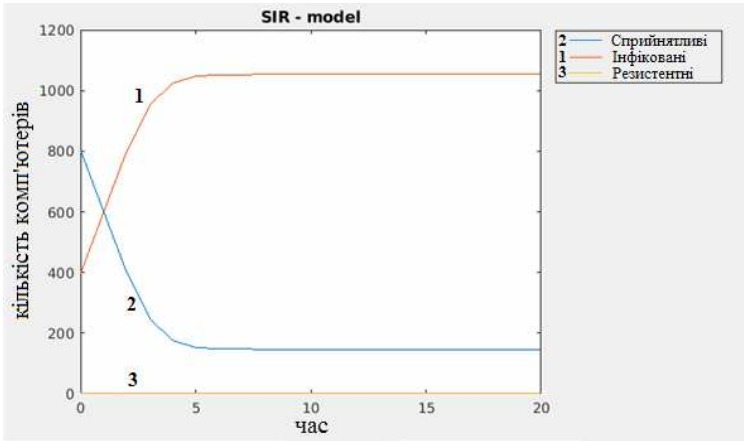


Рисунок 1 – Залежність кількості сприйнятливих та інфікованих вузлів від часу в моделі SIR без запізнювання

За допомогою методу кроків система із запізнюванням зводиться до системи звичайних рівнянь (без запізнювання), до якої застосовується метод Рунге – Кута 4-го та 5-го порядків.

Покладемо:

$$S = 800, I = 400, R = 0, N = S + I + R = 1200, \beta = 0,9,$$

$$\frac{1}{\gamma} = 0,01, \mu = 0,1, t = 20$$

Проаналізуємо як зміниться поведінка життєвого циклу вірусу при великих значеннях запізнювання $\tau(t)$. На рис. 2 бачимо, як змінюються чисельності сприйнятливих та інфікованих вузлів у випадку, коли запізнювання приймає значення від 50 до 150.

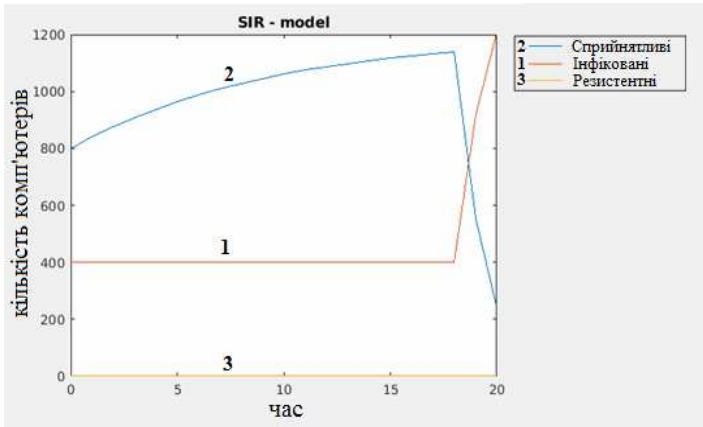


Рисунок 2 – Залежність кількості сприйнятливих та інфікованих вузлів від часу із запізнюванням у межах [50;150]

Якщо збільшити запізнювання до 200, то отримаємо результати, які зображено на рис. 3.

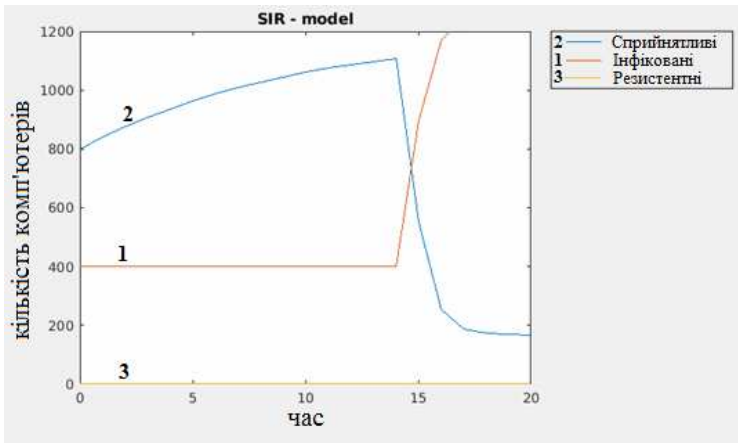


Рисунок 3 – Залежність кількості сприйнятливих та інфікованих вузлів від часу із запізнюванням 200

Порівнюючи із системою без введення запізнювання, можна помітити, що чим більше запізнювання, тим швидше зростає кількість інфікованих комп'ютерів. Це відбувається через те, що в інкубаційному

періоді вірус важче вирахувати та знешкодити антивірусом. Через відсутність групи резистентних індивідів комп'ютери переходять у інфіковану групу та виявляються під загрозою “вимирання”, на це впливає коефіцієнт μ .

Розглянемо також модель з трьох диференціальних рівнянь, яка відрізняється від попередньої тим, що вона містить ще й рівняння швидкості зміни кількості резистентних індивідів.

$$\begin{cases} \frac{dS(t)}{dt} = \frac{-\beta I(t-\tau(t))S(t-\tau(t))}{N} + \mu(N(t-\tau(t)) - S(t-\tau(t))), \\ \frac{dI(t)}{dt} = \frac{\beta I(t-\tau(t))S(t-\tau(t))}{N} - \gamma I(t-\tau(t)) - \mu I(t-\tau(t)), \\ \frac{dR(t)}{dt} = \gamma I(t-\tau(t)) \end{cases}$$

Розглянемо, як будуть змінюватися чисельності трьох груп індивідів при різних значеннях запізнювання та при фіксованих значеннях β, γ, μ .

Було отримано чисельний розв'язок цієї системи. Були задані невеликі значення запізнювання. Наприклад при запізнюванні $\tau(t)=5$ чисельності груп вузлів у комп'ютерній мережі змінюються, як зображено на рис. 4.

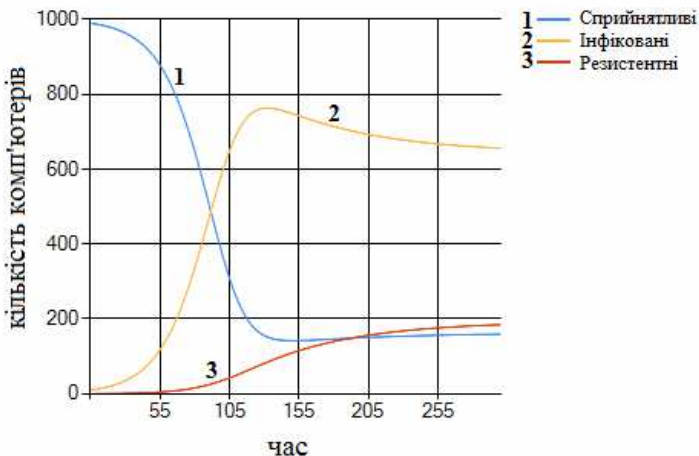


Рисунок 4 – Залежність кількості сприйнятливих, інфікованих та резистентних вузлів від часу із запізнюванням 5

Чисельний розв’язок системи при запізнюванні, що дорівнює 10, зображено на рис. 5.

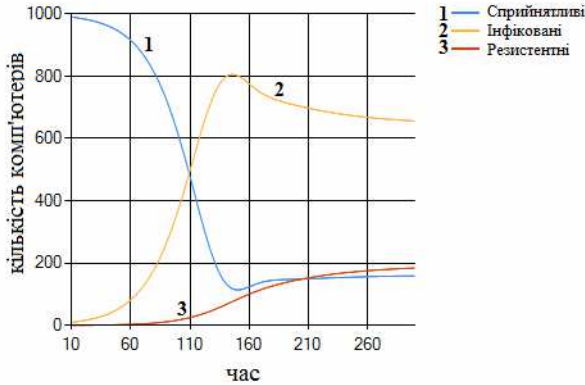


Рисунок 5 – Залежність кількості сприйнятливих, інфікованих та резистентних вузлів від часу із запізнюванням 10

Якщо збільшити величину запізнювання на 5, то отримаємо розв’язок, який зображено на рис. 6

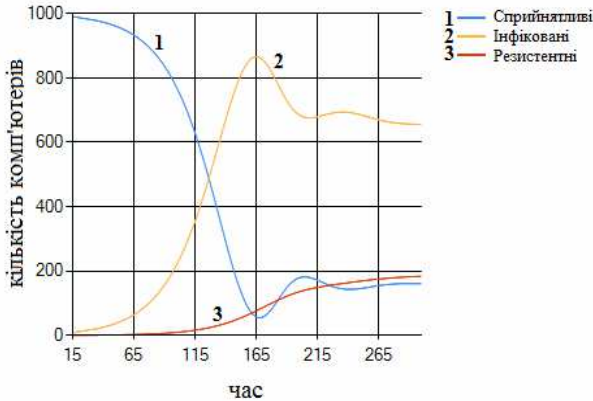


Рисунок 6 – Залежність кількості сприйнятливих, інфікованих та резистентних вузлів від часу із запізнюванням 15

Таким чином ми бачимо, що при невеликих значеннях запізнювання $\tau(t)$ зараження системи вірусом проходить не так активно, як при великих значеннях запізнювання. Це пояснюється тим, що своєчасно були застосовані відповідні заходи.

На певному інтервалі часу процес набуває коливального характеру. Амплітуда коливань збільшується зі збільшенням величини запізнювання. Але загальна тенденція перебігу епідемії зберігається.

У роботі [4] також досліджено модель розповсюдження комп'ютерних загроз, що описується системою трьох диференціальних рівнянь із запізнюванням. Але в ній, на відміну від цієї моделі, не враховуються не пов'язані з вірусом підключення та відключення вузлів у мережі.

Аналізуючи отримані результати, дійшли висновку, що для систем з невеликим запізнюванням процес стабілізується, кількість заражених комп'ютерів зменшується, вони переходять до лав вилікуваних. Період великих коливань залишається в минулому, мабуть спрацює антивірусна програма.

Висновки. У роботі було проведено дослідження динаміки розповсюдження комп'ютерних вірусів, розглянуто зміну характеру перебігу епідемії при різних значеннях запізнювання. Було встановлено, що чим менше значення запізнювання, тим менш активно проходить процес зараження вірусом системи.

Бібліографічні посилання

1. Kermack W. O., McKendrick A. G. A Contribution to the Mathematical Theory of Epidemics // Proceedings of the Royal Society. 1927. P. 700–721.
2. Tackeuchi Y., Wanbiao M., Hara T., Beretta E. Global asymptotic stability of an SIR epidemic model with distributed time delay // Pergamon. 2001. P. 47.
3. Zhao J., Liu M., Wang W. Analysis of a delayed SIR model with exponential birth and saturated incidence rate // Scientific research. Online journal. 2013. N 4. P. 60–67.
4. Варех Н. В., Литвин Т. В. Диференціальні моделі із запізнюванням для прогнозування розповсюдження комп'ютерних загроз // Форум «ТАК»: телекомунікації, автоматика, комп'ютерно-інтегровані технології. 2016. С. 136–138.

Надійшла до редколегії 30.06.2017