УДК 517.9:519.6

В.М. БУЛАВАЦЬКИЙ
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *v_bulav@ukr.net*.

В.О. БОГАЄНКО
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *sevab@ukr.net*.

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ДРОБОВО-ДИФЕРЕНЦІАЛЬНОЇ ДИНАМІКИ КОМП'ЮТЕРНИХ ВІРУСІВ НА ОСНОВІ МОДЕЛІ З ПОХІДНИМИ КАПУТО КУСКОВО СТАЛОГО ПОРЯДКУ

Анотація. Розглянуто узагальнений дробово-диференціальний аналог відомих моделей динаміки поширення комп'ютерних вірусів, побудований з використанням похідних Капуто кусково сталого порядку. Розроблено комбіновану методику одержання числово-аналітичного розв'язку відповідної задачі Коші для нелінійної системи дробово-диференціальних рівнянь кусково сталого порядку. Наведено результати якісного аналізу умов коректності цієї задачі Коші, аналізу стійкості задачі за Уламом–Хаєрсом та деякі результати комп'ютерного моделювання дробової динаміки поширення комп'ютерних вірусів на основі розглянутої моделі комп'ютерної вірусології.

Ключові слова: динаміка поширення комп'ютерних вірусів, математичне та комп'ютерне моделювання, дробово-диференціальні математичні моделі, похідні Капуто кусково сталого порядку, нелінійні моделі, якісний аналіз, UH-стійкість.

ВСТУП

Відомо, що поширення мережевих епідемій набуває все більш загрозливих масштабів, призводячи, зокрема, і до суттєвого зростання матеріальних втрат. Отже, побудова ефективних систем антивірусного захисту комп'ютерних мереж, що ґрунтуються на результатах математичного моделювання поширення шкідливого програмного коду, є актуальною проблемою. При цьому за допомогою розроблених під сучасну пору математичних моделей поширення комп'ютерних вірусів та дослідження на їхній основі еволюції системи вивчають динаміку кількості заражених вузлів та відповідні умови поширення шкідливого коду [1–4]. Зазначимо, що нині для моделювання динаміки комп'ютерних вірусів нерідко використовують математичні моделі типу SIR, SEIR, SIES тощо [5–10]. Так, наприклад, у SIR-моделі [5] розглядають три стани: S — susceptible (схильний до інфікування), $\mathfrak{I}$ — infected (інфікований), R — recovered (той, що одужав). Модель SEIR (Susceptible-Exposed-Infected-Removed) є модифікацією SIR-моделі. У ній враховано можливу наявність деякого «інкубаційного періоду», під час якого вірус не завдає шкоди інфікованому вузлу. Протягом латентного періоду (E) вузол є зараженим, але не поширює вірус. Через деякий час він стає здатним до зараження інших ($\mathfrak{I}$) і далі стає «таким, що одужав» (R) [3]. У SIES-моделі [11] вивчають динаміку поширення комп'ютерних вірусів за наявності ефекту дії зовнішніх комп'ютерів. Уважають, що в будь-який момент часу комп'ютер є внутрішнім або зовнішнім, залежно від того, чи є він доступним у мережі «Інтернет», чи ні. У побудові математичної моделі процесу використано такі змінні величини [11]:

- $S(t)$ — кількість уразливих комп'ютерів на момент часу t;
- $\mathfrak{I}(t)$ — кількість інфікованих комп'ютерів у момент t;
- $E(t)$ — кількість зовнішніх комп'ютерів у момент t.

Сумарну кількість комп'ютерів у мережі на момент часу t визначають співвідношенням $N(t) = S(t) + \mathfrak{I}(t) + E(t)$.