ISSN 2786-7102 (Online). System Research in Energy. 2022. 1(70): 53–61
doi: https://doi.org/10.15407/srenergy2022.01.053

УДК 004.942:620.9

Владислав Хайдуров, к.т.н., ст. досл., https://orcid.org/0000-0002-4805-8880
Інститут загальної енергетики НАН України, вул. Антоновича, 172, 03150, м. Київ, Україна
e-mail: info@ienergy.kiev.ua
Автор-кореспондент: allif0111@gmail.com

СТОХАСТИЧНИЙ І ДИНАМІЧНИЙ ПІДХОДИ ПРИ МОДЕЛЮВАННІ ПРОЦЕСІВ ПОШИРЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ ЕНЕРГЕТИЧНИХ ОБ'ЄКТІВ ТА ЇХ СИСТЕМ

Анотація. *Бурхливий розвиток інформаційних технологій в умовах сьогодення дає можливість виконувати контроль та автоматизацію процесів на підприємствах і в установах для забезпечення коректної й ефективної роботи різних енергетичних систем. Математичний апарат, який використовується у програмному забезпеченні для таких об'єктів і систем, дає можливість виконувати керування їх станами у різних штатних умовах. Іноді виникають непередбачувані фактори у роботі об'єктів енергетики, які можуть призвести до глобальних катастроф не лише окремого регіону, а і всього людства. Одним із таких факторів є навмисне пошкодження логіки роботи програмного забезпечення, що керує усіма процесами енергосистеми, з метою терору або інших зловмисних цілей. Подібні фактори вимагають побудови моделей, за допомогою яких можна спрогнозувати ризики та масштаби збитків, а також отримати загальну оцінку затрат для захисту програмного забезпечення енергосистем від подібних зловмисних дій. Результатом роботи є оптимізаційна математична модель та відповідний опис реалізації комплексного програмного засобу моделювання поширення шкідливого програмного забезпечення в сучасних енергетичних об'єктах і системах. Розроблена оптимізаційна математична модель базується на використанні методів оптимізації функцій та функціоналів з обмеженнями у вигляді систем звичайних диференціальних рівнянь з заданими відповідними початковими умовами. Для розроблення модулів програмного забезпечення моделювання процесів на базі математичної моделі PSIDR були використані стохастичні популяційні методи, моделі та алгоритми для визначення параметра керування на кожному кроці за часом. Використання таких оптимізаційних методів й алгоритмів дає можливість розв'язувати більш складні завдання, які вимагають процедури прогнозування поширення процесів різного походження загалом. Розроблена математична модель полягає у мінімізації затрат на закупівлю антивірусних засобів для захисту відповідних систем у енергетичних об'єктах і системах.*
Ключові слова: шкідливе програмне забезпечення, прогнозування, оптимізація, стохастична модель, детермінована модель, клітинний автомат, об'єкти енергетики.

1. Вступ

В умовах сьогодення неможливо собі уявити реальне життя без використання сучасної комп'ютерної техніки, смартфонів, гаджетів та інших пристроїв. Використання персональних комп'ютерів і мобільних пристроїв у поєднанні з Internet стало невід'ємною частиною повсякденного життя. Постійне використання Internet спричинило багато серйозних загроз конфіденційності та безпеці персональних даних одного або кількох користувачів. З кожним роком спостерігається суттєве збільшення кібератак з посиленням їх складності. Такі атаки впливають на електронні ресурси урядів, підприємств та окремих фізичних або юридичних осіб, а також завдають їм серйозні фінансові й соціальні збитки. Жодна особа не забезпечена стовідсотковим захистом від ураження власного пристрою шкідливим програмним забезпеченням (ШПЗ). Для комерційних фірм та / або банківських систем потрібно розуміти рівень збитків з плином часу, які отримуються в результаті роботи ШПЗ у конкретній сфері. У зв'язку з цим, питання прогнозування поширення ШПЗ у мережах та питання міри реагування у разі потрапляння ШПЗ у мережу компаній або фірм ставиться досить гостро.

Оцінка рівня збитків вимагає врахування багатьох факторів, але у першу чергу це стосується питання оцінювання динаміки поширення ШПЗ в комп'ютерних мережах. Це питання носить досить загальний характер, оскільки епідемії в людських спільнотах давно існують, як фактор загрози для людей і приносять величезні збитки. Відтак епідеміологія накопичила значний багаж моделей динаміки епідемій та оцінки на збитків

від них. Існує численна література з цієї тематики, зокрема [1–3]. І тому варто врахувати цей накопичений досвід. При цьому необхідно врахувати, що епідемії в комп'ютерних мережах мають відрізнятися від епідемій в людських спільнотах та економіці [3–5]. Застосування моделей з епідеміології для комп'ютерних мереж має бути критично переосмислене, крім того мають бути запропоновані нові підходи [6, 7].

2. Методи та матеріали

Задача прогнозування та задача оптимізації досить часто між собою пов'язані. Для проведення ефективного прогнозування у будь-якій сфері потрібно мінімізувати помилки на тих даних, що подаються у вигляді статистки [8, 9].

Нижче у даному розділі проведено аналіз деяких існуючих моделей прогнозування поширення ШПЗ та виконаний опис різних методів й алгоритмів, математичних основ, які засновані на статистичному опрацюванні даних, а також засновані на градієнтних методах пошуку екстремумів багатовимірних функцій [10–12]. Ефективне прогнозування, зокрема, прогнозування поширення ШПЗ у реальних об'єктах і системах, вимагає використання актуальних методів машинного навчання, у тому числі методів оптимізації.

2.1. Математичні моделі та програмний комплекс моделювання поширення шкідливого програмного забезпечення

Для розроблення комплексного програмного застосунку моделювання поширення шкідливого програмного забезпечення використовують кілька підходів. Перший підхід полягає у використанні модифікації класичних детермінованих моделей (ДМ) для дослідження стану поширення епідемій шкідливого програмного забезпечення. Другий підхід є більш універсальним – моделювання поширення ШПЗ на базі стохастичних моделей (СМ), наприклад, з використанням випадкових процесів, ланцюгів Маркова, клітинних автоматів, нейронних мереж тощо [5, 6]. Нижче описані моделі на базі класичних систем звичайних диференціальних рівнянь (СЗДР) та задач Коші для них, а також загальні принципи моделювання даних задач з використанням класичних клітинних автоматів з використанням різних околів – окіл Неймана та окіл Мура.

2.1.1. Детерміновані математичні моделі задачі поширення шкідливого програмного забезпечення

Модель поширення шкідливого програмного забезпечення SIR. У якості базової математичної моделі взято класичну модель SIR [8, 9]. Дана модель може описувати поширення багатьох різних процесів, причому ці процеси можуть бути як фізико-технічні, так і біологічні або економічні.

Нехай у нас є деяка мережа, яка поєднує кілька комп'ютерів. Це може бути локальна мережа, або мережа, яка має вихід на глобальні ресурси мережі Internet. Зрозуміло, що занесення ШПЗ в один персональний комп'ютер може призвести до поширення цього програмного забезпечення по всій мережі. Звісно ж, що швидкість поширення програмного забезпечення через дану мережу зумовлена різними факторами [6, 7]. До таких факторів можна віднести, наприклад:

– активність користувачів у даній мережі;

– цільова спрямованість програмного забезпечення та швидкість його поширення, яка керується програмним кодом, з якого він складається;

– комбінація факторів;

– інші фактори.

Будемо вважати, що цільові вузли мережі можуть бути в одному з трьох заданих станів:

– незаражені вузли мережі, які можуть бути піддані занесенню до них ШПЗ. Позначимо їх як S – susceptible;

– інфіковані вузли мережі, тобто такі, до яких вже занесли ШПЗ. Щодо роботи таких вузлів потрібно приймати негайні міри щодо збереження (у тому числі цілісності, за можливості) даних на таких вузлах. Позначимо їх як I – infective;

– стійкі до зараження вузли мережі, тобто такі, на яких встановлені відповідні міри захисту, (наприклад, мережеві екрани, антивірусні системи тощо), причому у таких вузлах видалене відповідне ШПЗ. Такі вузли позначимо як R – removed.

Процес поширення ШПЗ залежить лише від кількох параметрів:

– загальна кількість вузлів системи, яка поділяється на кількість незаражених вузлів, кількість інфікованих вузлів та кількість відновлених (несприятливих) вузлів у конкретній мережі;

– швидкість поширення ШПЗ;

– швидкість відновлення вузлів мережі у разі потрапляння у нього конкретного ШПЗ (швидкість реагування та прийняття відповідних захисних мір щодо лікування вузлів мережі).

Передбачається, що кількість вузлів мережі постійна протягом всього терміну дослідження цієї мережі. Це означає, що вузли не додаються до мережі і не видаляються з неї. Математично дана модель описується так.

Нехай N – загальна кількість комп'ютерів (вузлів) у мережі:

$$S(t)+I(t)+R(t)=N.$$

Зміна станів мережі можна описати у вигляді СЗДР, яка має вигляд:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\dfrac{-\beta I(t)}{N} S(t), \\ \dfrac{dI(t)}{dt} = \dfrac{\beta I(t)}{N} S(t) - \sigma I(t), \\ \dfrac{dR(t)}{dt} = \sigma I(t), \\ \dfrac{dS(t)}{dt} + \dfrac{dI(t)}{dt} + \dfrac{dR(t)}{dt} = 0. \end{cases} \quad (1)$$

У системи диференціальних рівнянь (1) β – швидкість зараження вузлів системи, а σ – швидкість лікування вузла системи (швидкість прийняття мір щодо забезпечення захисту вже інфікованого вузла системи).

Для відтворення динаміки математичної моделі (1) задано початкові умови виду:

$$S(0) = S_0,\ I(0) = I_0,\ R(0) = R_0. \quad (2)$$

Тепер математична модель (1) разом з початковими умовами (2) до неї задає задачі Коші, яка може бути розв'язана звичайними наближеними методами, наприклад, методами Ейлера або методами Рунге-Кутти.

Модель поширення шкідливого програмного забезпечення SAIR. На відміну від моделі *SIR*, у даній моделі усі вузли комп'ютерної мережі поділені на 4 фіксовані категорії:

– кількість неінфікованих вузлів (персональних комп'ютерів) мережі, які можуть бути інфікованими, позначимо як *S*;

– кількість вузлів мережі (персональних комп'ютерів), які мають встановлену систему захисту, наприклад, антивірусну систему, позначимо як *A*;

– кількість інфікованих вузлів мережі (персональних комп'ютерів) позначимо як *I*;

– кількість вузлів (персональних комп'ютерів) мережі, які вилікували, позначимо як *R*;

Поширення процесу інфікування елементів комп'ютерної мережі може бути подано у вигляді СЗДР так:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\dfrac{-\beta I(t)}{N} S(t), \\ \dfrac{dI(t)}{dt} = \dfrac{\beta I(t)}{N} S(t) - \sigma I(t), \\ \dfrac{dR(t)}{dt} = \sigma I(t), \\ \dfrac{dS(t)}{dt} + \dfrac{dI(t)}{dt} + \dfrac{dR(t)}{dt} = 0. \end{cases} \quad (2)$$

У моделі (3) також слід врахувати початкові умови типу (2), але для вузлів усіх 4-х станів з метою запуску процесу прогнозування поширення ШПЗ у відповідній мережевій системі.

Також слід зазначити, що у моделі (3): N – загальна кількість доданих нових вузлів у дану мережу; μ – частота вилучення вузлів системи, які неможливо відновити з причин, які не пов'язані з результатами дії ШПЗ; β_{SI} – частота зараження ШПЗ сприятливих вузлів мережі; β_{AI} – частота зараження вузлів системи, на яких встановлені системи захисту типу антивірусних систем або мережевих екранів; δ – частота, з якою вузли, які піддались впливу ШПЗ, виходять з ладу; σ_{IS} – частота лікування об'єктів (вузлів) мережі, які були заражені; σ_{RS} – частота лікування інфікованих вузлів системи (мережі) з участю оператора; α – інтенсивність звертання сприятливих до тих, які встановлюють систему захисту. Якщо взяти до уваги той факт, що до даної мережі не додають нові вузли, а вже існуючі вузли мережі виходять з ладу лише через вплив ШПЗ, тобто $N = \mu = 0$, то математична модель поширення ШПЗ набуває вигляду:

$$\begin{cases} \dfrac{dS}{dt} = -\alpha SA - \beta_{SI} SI + \sigma_{IS} I + \sigma_{RS} R, \\ \dfrac{dI}{dt} = \beta_{SI} SI + \beta_{AI} AI - \sigma_{IS} I - \delta I, \\ \dfrac{dR}{dt} = \delta I - \sigma_{RS} R, \\ \dfrac{dA}{dt} = \alpha SA - \beta_{AI} AI. \end{cases} \quad (4)$$

Для системи виду (4) також задаються початкові умови виду (2) для всіх 4-х станів вузлів у комп'ютерній мережі.

Модель поширення шкідливого програмного забезпечення PSIDR. Будь-яка математична модель, яка описує деякий процес, систему або комплекс роботи систем має враховувати багато факторів.

Математична модель передбачає два основні етапи. Перший етап полягає у тому, що ШПЗ поширюється досить швидко і вільно, тобто вузли комп'ютерної мережі мають лише два стани – *S* та *I*.

Другий етап передбачає процедуру реагування на наявне ШПЗ в комп'ютерній мережі. Протягом деякого проміжку часу ШПЗ у мережі ідентифікується. Далі виконується процедура лікування вузлів (персональних комп'ютерів) мережі. Тобто всі комп'ютери, які не були інфіковані автоматично «вакцинуються», тобто накладається на них підвищена система захисту.

Вузли системи, які вже були заражені, формують так званий «імунітет» і виліковуються від занесеного до них ШПЗ. Як і раніше, присутні у математичній моделі два параметри, які характеризують швидкість поширення ШПЗ – параметр μ та швидкість лікування вузлів мережі – це параметр швидкості δ.

У математичній моделі *PSIDR* через *I* позначено загальну кількість інфікованих елементів (вузлів) комп'ютерної мережі. Ці елементи мережі є поширювачами ШПЗ. *S* – загальна кількість неінфікованих вузлів комп'ютерної мережі. Ці вузли мережі можуть бути піддані зараженню протягом всього часу існування у даній мережі. *R* – загальна кількість вилікуваних елементів комп'ютерної мережі. Ці вузли мають так званий «імунітет» до зараження. Останній тип вузлів у системі – це *D* – загальна кількість знайдених інфікованих об'єктів у системі комп'ютерної мережі.

Опис наведений вище дає змогу записати відповідну математичну модель прогнозування поширення ШПЗ у даній мережі. Математична модель має такий вигляд:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\beta S(t) I(t) - \mu S(t), \\ \dfrac{dI(t)}{dt} = \beta S(t) I(t) - \mu I(t), \\ \dfrac{dR(t)}{dt} = \sigma D(t) + \mu S(t), \\ \dfrac{dD(t)}{dt} = \mu I(t) - \sigma D(t), \\ \dfrac{dS(t)}{dt} + \dfrac{dI(t)}{dt} + \dfrac{dR(t)}{dt} + \dfrac{dD(t)}{dt} = 0. \end{cases} \quad (5)$$

У математичній моделі (5) присутні три параметри, що характеризують швидкості, зокрема: β – швидкість інфікування вузлів мережі; σ – швидкість лікування вузлів мережі; μ – швидкість ідентифікації вузлів мережі зі ШПЗ. Особливістю даної моделі є те, що антивірусний захист повинен бути оновлений якомога раніше, оскільки затримка оновлення антивірусного захисту у кожному вузлу мережі призводить до більшого поширення ШПЗ у даній мережі.

Для математичної моделі (5) задаються початкові умови виду:

$$I(0) = I_0, S(0) = S_0, D(0) = R(0) = 0. \quad (6)$$

У такому разі ми отримуємо задачу Коші виду (5)–(6), яка також може бути розв'язана будь-яким явним наближеним методом, наприклад, методом Ейлера або методо Рунге-Кутти. Для знаходження наближеного розв'язку задачі Коші (5)–(6) використано класичний метод Ейлера. У третьому розділі наведено основі результати розроблення модулів, які відтворюють роботу моделі виду (5)–(6).

2.1.2. Стохастична модель поширення шкідливого програмного забезпечення

Клітинні автомати. Моделі будь-яких складних реальних систем та їхніх комплексів, а також імітаційні моделі мають високу цінність завдяки задачам прогнозування фізико-технічних, економічних, екологічних, соціальних та інших процесів. Прогнозування поширення ШПЗ досить схоже на прогнозування поширення епідеміологічних процесів. Епідеміологічні події, спричинені вірусами, забруднення від стаціонарних джерел забруднюючих речовин або нові різновиди біотероризму можуть спричинити значні затрати людей та їхніх ресурсів. З даної причини важливо вивчати та моделювати поширення збудників у популяції.

Клітинний автомат (*КА*) – це абстрактний об'єкт, який складається з множини комірок, кожна з яких має певний скінченний стан. Стан може змінюватись з часом, виходячи з конкретних умов, які описують той чи інший процес поширення явища.

Комірка – це окремий елемент клітинного простору, або так звана «найменша одиниця простору».

Клітинний простір – це простір решітки, яка складається з комірок, і кожна клітинка знаходиться в одному з кількох попередньо визначених станів.

Правило стану КА – це правило, що регулює перехід між комірками та їх станами. Особливе значення мають визначення найбільш відповідні правила переходу для досліджуваного явища або процесу.

Визначення кінцевого автомата клітинки називається «локальним», оскільки воно використовує лише околиці як вхідні дані. Сусідство відноситься до клітин, що оточують певну клітину, і вони мають здатність впливати на наступний стан цієї клітини. Вибір сусідства впливає на поведінку клітинного простору. Вибір відповідного сусідства залежить від співвідношення між елементами.

Найважливішими типами околів є околи фон Неймана та околиці Мура (рис. 1).

На практиці використовується більша кількість околів та сіток, але на рис. 1 наведені ті, які використані при розробленні програмного забезпечення моделювання поширення ШПЗ у мережі.

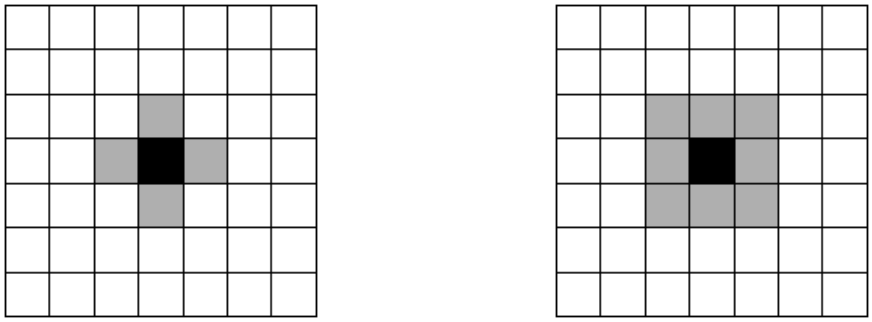

Рис. 1. Околи клітинки у двовимірному просторі КА: ліворуч – окіл фон Неймана; праворуч – окіл Мура

Метод Монте Карло. Імовірнісні методи моделювання активно використовуються для вивчення впливу випадкової мінливості різних величин на властивості машин, на хімічні або біологічні процеси, на несучу здатність або надійність конструкції та в багатьох інших випадках. Дуже потужним інструментом дослідження випадкових процесів є метод Монте-Карло. Єдина інформація, яка потрібна, це співвідношення між вихідною та вхідною величинами, зокрема, у такому вигляді:

$$y = f\left(x_1, x_2, \cdots, x_n\right). \tag{7}$$

Метод повторює випробування з генерованими комп'ютером випадковими числами, обробленими відповідними математичними операціями. У кожному «випробуванні» вхідним змінним x_1, x_2, …, x_n присвоюються випадкові значення, але такі, щоб їхні розподіли відповідали розподілу ймовірностей кожної змінної. З цими значеннями вихідна величина *y* розраховується за рівнянням (7).

Ефективність даного підходу базується за псевдовипадкових числах, які реалізовані у обчислювальних комплексах.

Створення випадкових чисел із заданими розподілами. Сучасні прикладні програмні забезпечення пропонують досить часто використовувати розподіли, наприклад, однорідні або звичайні. Випадкові числа, що відповідають іншим аналітично визначеним розподілам, можуть бути згенеровані за допомогою рівномірного розподілу.

2.2. Математична модель мінімізації збитків від поширення шкідливого програмного забезпечення

Для побудови моделі оптимального керування розглянемо ДМ PSIDR, яка була описана у розділі 2.1 даної роботи. У моделі оптимального керування будемо вважати, що параметр μ є параметром керування і він є обмеженим. Матимемо задачу оптимізації, яка описана у математичному формулюванні нижче.

Нехай є функціонал поданого нижче виду:

$$J\left(\mu(t)\right) = \int_0^T \left(A \cdot I\left(\mu(t)\right) + \right.$$
$$\left. + B \cdot D\left(\mu(t)\right)\right) dt \to \min, \tag{8}$$

де

A – платня за персональні комп'ютери / ноутбуки, які були пошкоджені ШПЗ;

B – платня за оновлення антивірусної системи для персональних комп'ютерів та / або ноутбуків, які досліджуються;

T – кінцевий час, протягом якого виконувалось дослідження поведінки ШПЗ у персональних комп'ютерах / ноутбуках.

З точки зору практики є очевидним те, що можливості встановлення нового антивірусного засобу є обмеженими, тобто $0 \le \mu(t) \le M$.

Тоді задача керування описується такою математичною моделлю. Знайти глобальний мінімум функціоналу (8) з урахуванням обмеження, яке описується у вигляді самої моделі PSIDR, тобто у вигляді задачі Коші для СЗДР:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\beta S(t) I(t) - \mu(t) S(t), \\ \dfrac{dI(t)}{dt} = \beta S(t) I(t) - \mu(t) I(t), \\ \dfrac{dR(t)}{dt} = \sigma(t) D(t) + \mu(t) S(t), \\ \dfrac{dD(t)}{dt} = \mu(t) I(t) - \sigma(t) D(t). \end{cases} \tag{9}$$

Початкові умови задачі мають такий вигляд (6).

Обмеження на шуканий параметр керування має вигляд:

$$0 \le \mu(t) \le M. \tag{10}$$

Задачу, яка описується у вигляді математичної моделі (8)–(9)–(6) можна розв'язувати багатьма методами й алгоритмами. У більшості випадків подібні задачі не мають аналітичних розв'язків, а якщо і мають, то такі розв'язки не цікавлять,

оскільки реальні прикладні задачі сьогодення можуть бути розв'язані лише чисельно. До аналітичних методів пошуку параметра керування можна віднести принцип максимуму Понтрягіна. Програмна реалізація обмеження (задачі Коші) базуватиметься на використанні класичного методу Ейлера для задач Коші для ЗДР та СЗДР.

Для підвищення точності розв'язування прямої задачі на базі математичної моделі (8)–(9)–(6) з відомим параметром керування (10) можна використати методи типу Рунге-Кутти 2, 3, 4 та вищих порядків. Мінімізація функціоналу виду (8) проводиться з використанням детермінованих методів та популяційних (багатоагентних) стохастичних методів й алгоритмів.

3. Результати

Розроблений програмний комплекс складається з кількох модулів, кожний з яких має відповідний графічний інтерфейс користувача. Загальна структура програмного комплексу подана на рис. 2.

Структура розробленого програмного комплексу може бути модифікована додатковими модулями, оскільки кожен модуль працює незалежно від інших модулів програмного комплексу. На рис. 3 показано інтерфейс одного з моду-

Рис. 2. Структура програмного комплексу моделювання поширення шкідливого програмного забезпечення

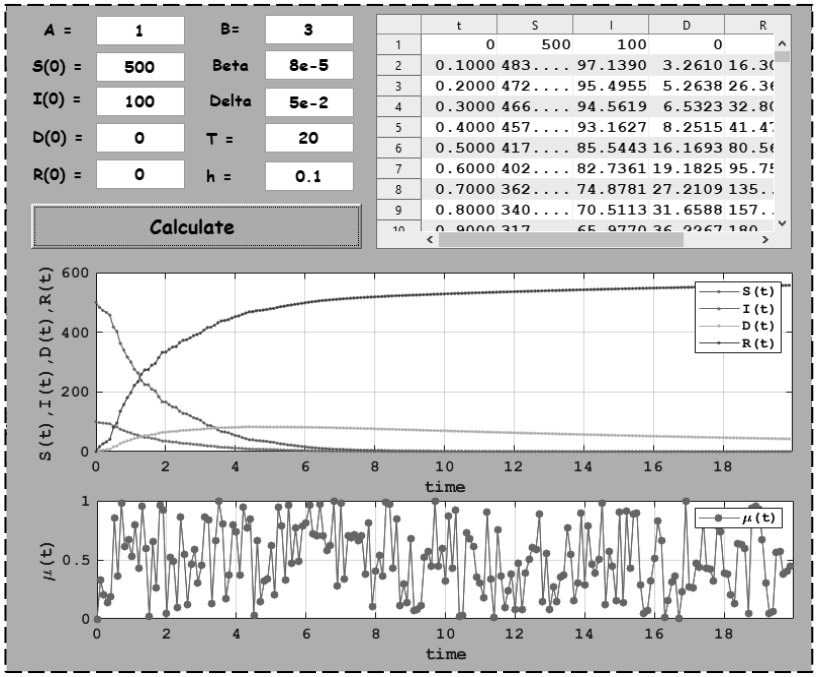

Рис. 3. Програмний інтерфейс модуля керування на базі моделі PSIDR

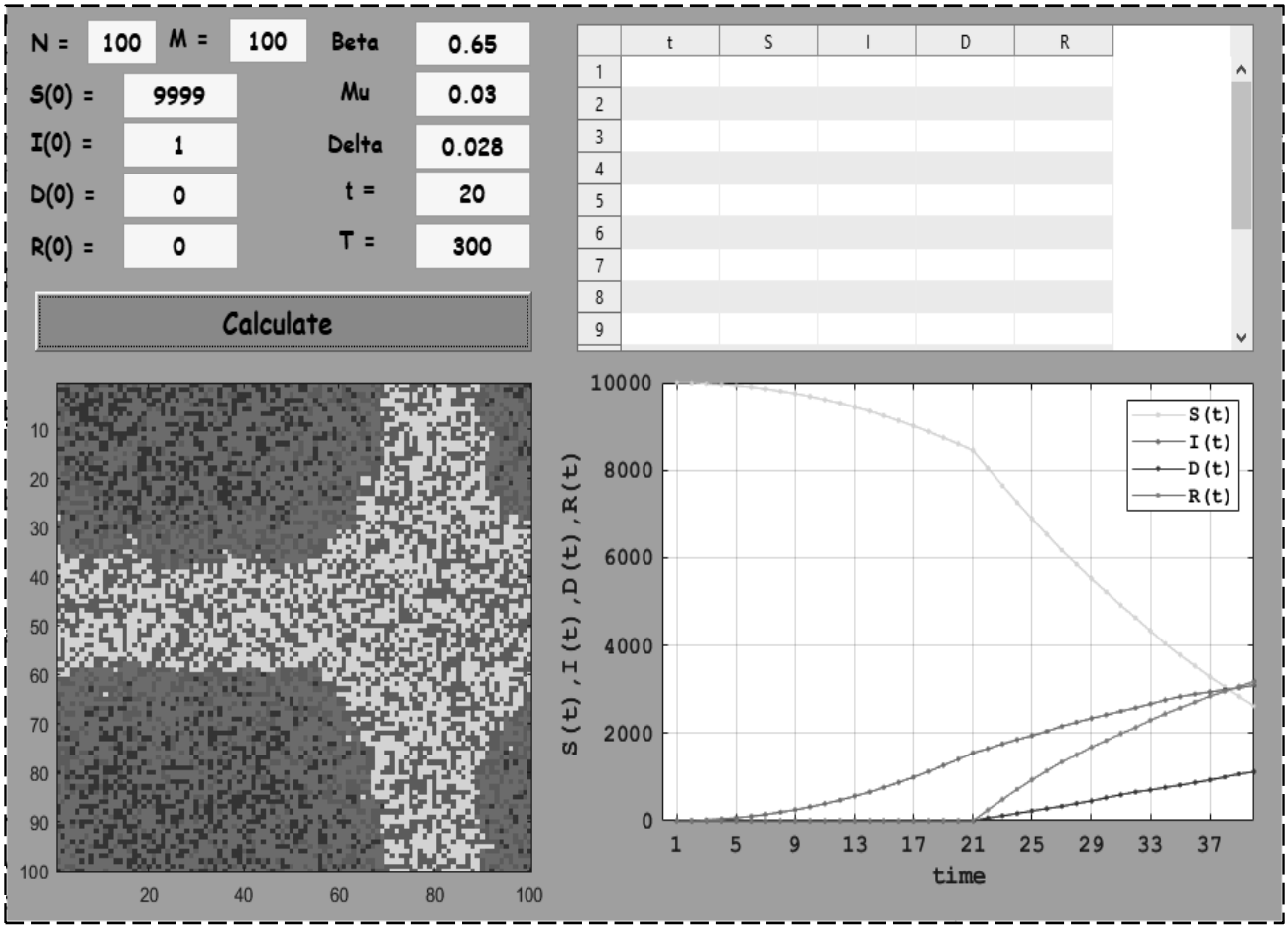

Рис. 4. Програмний інтерфейс модуля стохастичної моделі прогнозування поширення ШПЗ

лів комплексного програмного застосунку – реалізація моделі керування, яка передбачає мінімізацію загальних витрат на закупівлю та оновлення антивірусних систем програмного забезпечення, яке присутнє в сучасних енергетичних об'єктах і системах.

На рис. 4 показано програмний інтерфейс СМ моделювання поширення шкідливого програмного забезпечення.

Інтерфейс програми та його логічна частина реалізовані за принципом модульної структури у системі прикладної математики MATLAB.

Розроблений програмний комплекс можна модифікувати доопрацювавши відповідні моделі поширення шкідливого програмного забезпечення для особливих випадків ШПЗ, які можуть трапитись при роботі з інформаційними системами.

4. Обговорення

У ході проведення моделювання з використанням різних моделей визначено, що СМ більш адаптовані для моделювання процесів поширення ШПЗ. Ефективність СМ на базі КА проявляється в тому, що паралельно можна отримувати і статистику, яка ж присутня при використанні ДМ на базі диференціальних рівнянь та їх систем, і картину поширення самого процесу з масштабом у часі. Також перевагою СМ на базі КА є цілочисельність статистики, яка відсутня при моделюванні поширення ШПЗ з використанням ДМ на базі диференціальних рівнянь та їх систем. Недоліком СМ є порівняно довгий час роботи, який відведений на відпрацювання ДМ.

Слід також зазначити, що будь-які з реалізованих моделей можна досить швидко модифікувати з метою врахування усіх факторів, які впливають на процеси поширення ШПЗ загалом.

5. Висновки

Нинішні темпи розвитку комп'ютерних систем вимагають максимального для них захисту від шкідливого програмного забезпечення (ШПЗ). Потрапляння ШПЗ навіть до локальної інформаційної системи можуть призвести до серйозних наслідків, до яких можна віднести втрату даних користувачів

системи, вилучення даних з системи, підміну даних в цій системі, навіть фінансові втрати конкретної компанії, до якої належить відповідна система.

Для того, щоб максимально зменшити ризики формування різного роду неприємних та / або катастрофічних наслідків від впливу ШПЗ на ту або іншу систему, проводять різного роду моделювання, наприклад, імітаційне, яке дає змогу оцінити ступінь ризику та фінансові втрати, які можуть виникнути внаслідок дії ШПЗ.

Проведено порівняльний аналіз сучасних методів, засобів, програмного забезпечення для проведення моделювання поширення шкідливого програмного забезпечення. Обрано як середовище розробки відповідного програмного забезпечення систему прикладної математики MALTAB.

Розроблений програмний комплекс моделювання поширення ШПЗ складається з трьох основних програмних модулів: модуль прогнозування поширення ШПЗ на базі ДМ PSIDR, яка представляється у вигляді задачі Коші для СЗДР; модуль прогнозування поширення ШПЗ на базі СМ PSIDR, яка запрограмована на базі КА з використанням околів Неймана і Мура; модуль реалізації моделі керування для ДМ PSIDR, яка у свою чергу використовує популяційні (багатоагентні) стохастичні методи й алгоритми для мінімізації затрат на кожному кроці за часом.

Усі три програмні модулі комплексу протестовані й перевірені на різних вхідних даних (початкових умовах для моделювання поширення ШПЗ у системі). До кожного програмного модуля розроблений графічний інтерфейс користувача з можливістю проведення моделювання процесів для різних початкових умов.

Слід зазначити, що ДМ є менш гнучкими при моделюванні подібних завдань. Їх недолік проявляється у тому, що кількість досліджуваних об'єктів не завжди є натуральним числом, і у такому разі використовують округлення за класичними математичними правилами. Також процес модифікації ДМ є ускладнений у порівнянні з процесом модифікації СМ. СМ мають ще одну суттєву перевагу, яка полягає у наочності проходження процесу. Це дає більш чітке уявлення про сам процес і робить моделювання значно гнучкішим не лише для даного роду завдань.

Список посилань

1. Alexeev, A., Henshel, D.S., Cains, M., Sun, Q. (2016) On the malware propagation in heterogeneous networks. In: 2016 *IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob),* 1—5.
2. Brauer, F., Castillo-Chavez, C. (2012). Epidemic Models. In: Mathematical Models in Population Biology and Epidemiology. *Texts in Applied Mathematics, vol 40.* Springer, New York, NY. https://doi.org/10.1007/978-1-4614-1686-9_9.
3. Hernández Guillén, J.D., Martín del Rey, Á., Hernández Encinas, L. (2017). New Approaches of Epidemic Models to Simulate Malware Propagation. In: Pérez García, H., Alfonso-Cendón, J., Sánchez González, L., Quintián, H., Corchado, E. (eds) International Joint Conference SOCO'17-CISIS'17-ICEUTE'17 León, Spain, September 6–8, 2017, Proceeding. SOCO ICEUTE CISIS 2017 2017 2017. *Advances in Intelligent Systems and Computing, vol 649.* Springer, Cham. https://doi.org/10.1007/978-3-319-67180-2_61.
4. Kuniya, T. (2021) Structure of epidemic models: toward further applications in economics. *JER 72*, 581—607. https://doi.org/10.1007/s42973-021-00094-8.
5. Karyotis, V., & Khouzani, M. (2016) Malware Diffusion Models for Modern Complex Networks: Theory and Applications. Morgan Kaufmann, Amsterdam.
6. Liu, W., Liu, C., Liu, X., Cui, S., Huang, X. (2016) Modeling the spread of malware with the influence of heterogeneous immunization. *Appl. Math. Model. 40(4),* 3141—3152.
7. Peng, S., Yu, S., & Yang, A. (2014) Smartphone malware and its propagation modeling: a survey. *IEEE Commun. Surv. Tutorials 16(2),* 925—941.
8. Galchynsky, L, & Pushko, A. (2018) Modeling the cost estimation of preventive strategies to combat the spread of infectious diseases. A *Young Scientist, vol 4(1).* 120—124.
9. Galchynsky, L, & Pushko, A. (2018) Cost-Effectiveness of Specifying Control Parameters as Functions in Cost-Estimating Modeling of Preventive Strategies to Control Epidemics. *International economic relations and the world economy. Vol. 19(1*). 56—59.
10. Khaidurov V., Tsiupii T., Zhovnovach T. (2021) Modelling of Ultrasonic Testing and Diagnostics of Materials by Application of Inverse Problems. ITTAP'2021: *1nd International Workshop on Information Technologies: Theoretical and Applied Problems. ITTAP'2021: November 16–18, 2021.* 1—5.
11. Khaidurov V., Zaporozhets A., Tsiupii T. (2021) Optimization models of industrial furnaces and methods for obtaining their numerical solution. Springer, *Systems, Decision and Control in Energy II. Studies in Systems, Decision and Control, vol. 346,* 121—139. https://doi.org/10.1007/978-3-030-69189-9_7.
12. Khaidurov V., Zaporozhets A., Tsiupii T. (2022) Creation of High-Speed Methods for Solving Mathematical Models of Inverse Problems of Heat Power Engineering. Springer, *Systems Decision and Control in Energy III, vol. 399,* 41—74. https://doi.org/10.1007/978-3-030-87675-3.

A STOCHASTIC AND DYNAMIC APPROACH IN SIMULATING SPREAD PROCESSESS OF MALWARE OF AUTOMATED ENERGY FACILITIES AND THEIR SYSTEMS

Vladyslav Khaidurov, PhD (Engin.), Senior Researcher, https://orcid.org/0000-0002-4805-8880
Institute of General Energy of NAS of Ukraine, 172, Antonovycha Str., 03150, Kyiv, Ukraine
e-mail: info@ienergy.kiev.ua
Corresponding author: allif0111@gmail.com

Abstract. *The rapid development of information technologies in today's conditions makes it possible to control and automate processes and enterprises, institutions to ensure the correct and efficient operation of various energy systems. The mathematical apparatus used in the software for such objects and systems makes it possible to manage their states in various regular conditions. Sometimes unpredictable factors arise in the operation of energy facilities, which can lead to global catastrophes not only for a particular region, but also for all of humanity is the deliberate damage to the logic of the software that controls all the processes of the power system is one of these factors, for the purpose of terror or other malicious purposes. Such factors require the construction of models with which it is possible to predict the scale of risk and extent of damage, as well as to obtain a general estimate of the costs of protecting power system software against such malicious actions. An optimization mathematical model and a corresponding description of the implementation of a complex software tool for modeling the spread of malicious software (malware) in modern energy facilities and systems is the result of the work. The developed optimization mathematical model is based on the use of methods of optimization of functions and functionals with restrictions in the form of systems of ordinary differential equations with given corresponding initial conditions. To develop process simulation software modules based on the PSIDR mathematical model, stochastic population methods, models and algorithms were used to determine the control parameter at each time step. The use of such optimization methods and algorithms makes it possible to solve more complex tasks. It requires a procedure for predicting the spread of processes of various origins in general. The developed mathematical model consists in the minimization of costs for the purchase of antiviruses for the protection of relevant systems in energy facilities and systems.*
Keywords: malware, prediction, optimization, stochastic model, deterministic model, cellular automaton, energy objects.

Надійшла до редколегії: 15.09.2022