УДК 004.49:004.94

МОДЕЛЮВАННЯ РОЗПОВСЮДЖЕННЯ КОМП'ЮТЕРНИХ ВІРУСІВ НА ОСНОВІ ІМОВІРНІСНОГО КЛІТИНКОВОГО АВТОМАТУ

Микола Грайворонський, Ірина Стьопочкіна

В умовах зростання обсягів та видів шкідливого програмного забезпечення, яке узагальнено називають вірусами, актуальною задачею є моделювання його розповсюдження для прийняття запобіжних заходів. Існують моделі розповсюдження комп'ютерних вірусів у вигляді звичайних диференціальних рівнянь, але вони не приділяють належної уваги їх просторовому розповсюдженню та логічним особливостям, зосереджуючись на кількісних показниках. В даній статті розглянуто підхід до моделювання вірусів на основі клітинкового автомату, запропоновано нову модель розповсюдження вірусів, яка відрізняється можливістю враховувати деякі риси самовідтворення шкідливого ПЗ, бере до уваги дію антивірусного захисту та його вплив на розповсюдження зараження. Модель застосовано до ряду практичних прикладів, в результаті моделювання одержано інформацію щодо розподілу зараження мережею. Запропонована модель може бути адаптована до різних видів шкідливого ПЗ.

Ключові слова: *шкідливе програмне забезпечення, віруси, моделювання, клітинкові автомати*

Вступ

В сучасному інформаційному середовищі велику увагу останнім часом приділяють проблемам захисту цілісності інформації, порушення якої відбувається внаслідок дії різноманітного шкідливого програмного забезпечення, яке зазвичай узагальнено називають вірусами. З цього випливає цікавість до закономірностей розповсюдження вірусів, які постійно удосконалюються та видозмінюються зловмисниками [3].

Існує ряд робіт [4-6], присвячених аналізу розподілу співвідношення між так званими підозрілими, інфікованими та вилікованими (Susceptibles, Infectious, and Recovered) комп'ютерами. Відповідні дослідження використовують SIR–моделі, що представляють собою системи звичайних диференціальних рівнянь, які враховують різні фактори існування та розповсюдження вірусів. Такі моделі мають суттєвий недолік – розглядається еволюція кількості заражених станцій у часі, однак розподіл за простором залишається невідомим.

Відомо, що розповсюдження епідемій має схожі закономірності із розповсюдженням комп'ютерних вірусів [2, 6]. Цей підхід приводить до моделей у вигляді диференціальних рівнянь у часткових похідних, що дозволяє врахувати розподіл процесу як у часі, так і в просторі, однак він складно застосовується до реального випадку, коли слід врахувати, що простір логічних зв'язків між станціями мережі зазвичай представлений графом нерегулярної структури. GERT-моделі, що можуть вирішити цю проблему, теж мають ряд недоліків, пов'язаних із складністю одержання законів розподілу імовірнісних величин. Цікавими моделями, які широко застосовуються для моделювання багатьох явищ у дискретних середовищах із дискретним часом є скінчені клітинкові автомати [1], в яких кожен вузол знаходиться в одному із станів (кількість станів є скінченою), і може переходити в інший стан по визначеним правилам, які залежать від стану самого вузла та його оточення в попередній момент часу. Ці правила єдині для всіх вузлів, незмінні за часом та обробляються синхронно для всіх вузлів. Наразі клітинкові автомати почали використовуватись і в моделюванні епідемій [7].

У цій роботі запропоновано нову модель, що описує розповсюдження шкідливого програмного забезпечення, яке має функцію відтворення власних копій і розповсюдження їх на сусідні комп'ютери. В запропонованій моделі поєднано врахування факторів розповсюдження вірусів, які зазвичай враховуються в SIR-моделях, із представленням моделі розповсюдження вірусів одного класу на основі клітинкового автомату з імовірнісними правилами переходів, що дає змогу враховувати як часові, так і просторові характеристики процесу, та його дискретний характер. Перевагою моделі є й врахування деяких характеристик політики антивірусного захисту, що можуть якісно вплинути на розповсюдження вірусів.

Постановка задачі

Необхідно виявити основні закономірності розповсюдження комп'ютерних вірусів, та представити ці закономірності у моделі розповсюдження вірусів на основі клітинкового автомата. Змоделювати в часі та в просторі розповсюдження вірусу в мережі. Час є дискретним, просторове розподілення комп'ютерів один стосовно одного вважаємо відомим. Під просторовим розподіленням маємо на увазі розподілення логічних звязків між машинами, причому сусідами вважаються ті машини, які є наявними у переліку адрес, чи можуть безпосередньо обмінюватись даними через мережу. Зокрема, необхідно врахувати такі основні фактори:

Спосіб розповсюдження (безпосереднє зараження шляхом передачі заражених файлів мере-

жею, чи зараження через пошту, коли вірус самостійно розсилається усім комп'ютерам, наявним у списку контактів, однак користувач має його активізувати).

Залежність від платформи (віруси, що орієнтовані на конкретну операційну систему, як правило, не можуть діяти на станціях із іншими операційними системами).

Наявність та частота поновлень антивірусного забезпечення.

Опис моделі розповсюдження комп'ютерних вірусів абстрактною мережею

Нехай задано логічну структуру мережі, комп'ютери якої поєднані між собою зв'язками. Відомий граф зв'язків між комп'ютерами (безпосередній зв'язок «сусідів», зв'язок через пошту (індикатор такого зв'язку – наявність «сусіда» у списку контактів)).

Вірус, потрапивши на комп'ютер, може заразити його, а також на наступних кроках додатково заразити інші комп'ютери, з якими даний має зв'язки.

Комп'ютери можуть бути ввімкненими та вимкненими. Якщо комп'ютер ввімкнений (активний), його взаємодія із вірусом відбувається за правилами, наведеними нижче.

Вимкнений комп'ютер перебуває в пасивному стані, а коли вмикається, задовольняє тим самим правилам, що й активний комп'ютер. Також вимкнений комп'ютер може зберігати інформацію, що дійшла до нього (вірус, який передався від сусіда, або оновлення баз антивіруса – це аналог того, що при включені користувач оновить бази антивіруса).

Введемо такі атрибути, що характеризують стан комп'ютера:

I – комп'ютер був заражений;

V – на комп'ютер потрапив вірус, однак не заразив його;

R – вірус пересилається далі з даного комп'ютера;

O – на комп'ютері встановлено ОС визначеного типу;

A – комп'ютер захищений антивірусним забезпеченням;

A_0 – комп'ютер захищений антивірусним забезпеченням, однак бази застарілі;

H – комп'ютер вилікувався від вірусу після встановлення останніх оновлень антивірусу.

Нехай ввімкнений комп'ютер може перебувати в одному з 7-ми станів, які характеризуються наступною сукупністю атрибутів:

$$O \wedge A \wedge \neg I ; \quad (1)$$

$$O \wedge (\neg A \vee A_0) \wedge \neg I ; \quad (2)$$

$$O \wedge (\neg A \vee A_0) \wedge I ; \quad (3)$$

$$O \wedge I \wedge (\neg A \vee A_0) \wedge R ; \quad (4)$$

$$O \wedge (\neg A \vee A_0) \wedge V ; \quad (5)$$

$$O \wedge V \wedge (\neg A \vee A_0) \wedge R ; \quad (6)$$

$$O \wedge H . \quad (7)$$

До кожного з цих станів можна дописати «доповнюючий» (в залежності від типу ОС):

$$\neg O \wedge A \wedge \neg I ; \quad (1a)$$

$$\neg O \wedge (\neg A \vee A_0) \wedge \neg I ; \quad (2a)$$

$$\neg O \wedge (\neg A \vee A_0) \wedge I ; \quad (3a)$$

$$\neg O \wedge I \wedge (\neg A \vee A_0) \wedge R ; \quad (4a)$$

$$\neg O \wedge V \wedge (\neg A \vee A_0) ; \quad (5a)$$

$$\neg O \wedge V \wedge (\neg A \vee A_0) \wedge R ; \quad (6a)$$

$$\neg O \wedge H . \quad (7a)$$

Переходи між станами відбуваються у дискретні моменти часу. Стан клітинки (комп'ютера) в наступний момент часу залежить від стану клітинки в попередній момент та станів сусідів.

Правила, які відображають цю залежність, представлено в табл.1. Сусідами вважаються будь-які два комп'ютера, якщо адреса одного є у переліку адрес іншого.

Таблиця 1

Переходи, які змінюють стан клітинки

№ переходу	**Стани сусідів**	**Стан клітинки в попередній момент S_{prev}**	**Стан клітинки в наступний момент S_{next}**
1	Хоча б один сусід заражений, передає вірус, і має ОС визначеного типу (знаходиться в стані (4))	Не заражений, не захищений або бази АВЗ застарілі, має ОС визначеного типу (стан (2))	Заражений (стан (3))
2	Хоча б один сусід передає вірус і має ОС визначеного типу (знаходиться в стані (4) або (6))	Не заражений, не захищений або бази АВЗ застарілі, і має іншу ОС (стан (2))	Вірус потрапив на комп'ютер, однак ще не активований (стан (5))

Продовження таблиці 1

№ переходу	**Стани сусідів**	**Стан клітинки в попередній момент S_{prev}**	**Стан клітинки в наступний момент S_{next}**
3	Сусіди знаходяться в будь-якому стані	Заражений, не захищений або бази АВЗ застарілі, має ОС визначеного типу (стан (3))	Заражений, не захищений або бази АВЗ застарілі, має ОС визначеного типу та передає вірус сусідам (стан (4))
4	Сусіди знаходяться в будь-якому стані	Вірус потрапив на комп'ютер, однак ще не активований (стан (5))	Заражений, не захищений або бази АВЗ застарілі, має ОС визначеного типу (стан (3))
5	Хоча б один сусід заражений, передає вірус і має ОС іншого типу (стан (3а))	Не заражений, не захищений, має ОС визначеного типу (стан (2))	Вірус потрапив, однак не заразив (стан 5)
6	Сусіди знаходяться в будь-якому стані	Заражений, не захищений або має застарілі бази АВЗ (стан (3))	Через n кроків – зцілений, захищений (стан (7))
7	Хоча б один сусід передає вірус і має ОС визначеного типу (знаходиться в стані (4) або (6))	Не заражений, не захищений або має застарілі бази АВЗ (стан (3))	Вірус неактивний, однак внаслідок необережності користувача розсилається іншим користувачам (стан (6))
Антивірусний захист			
8	Сусіди знаходяться в будь–якому стані	Заражений, передає вірус і має ОС визначеного типу (стан 4)	Через n кроків, де n - заданий параметр – зцілений, захищений (стан (7))
9	Хоча б один із сусідів знаходиться в стані (1)	Знаходиться в стані (3), (4) або (5)	Перехід до стану (1)

Примітки.

1. Припускається, що заражений комп'ютер може бути лише за умов: а) застарілого антивірусного захисту (АВЗ), б) відсутності АВЗ.

2. Стан (7) (*H* – зцілений, захищений) настає внаслідок поновлення АВЗ. Після того, як стан *H* досягнутий, зараження неможливе, оскільки поновлене АВЗ розпізнає даний тип вірусу.

3. Зцілення відбувається миттєво, одночасно з поновленням АВЗ.

4. Стан (6) можливий, коли користувач ненавмисно надсилає файли, заражені неактивованим вірусом.

5. З урахуванням табл.1 можливі такі переходи між станами, які змінюють стан клітинки:

$$
\begin{gathered}
(2)\to(3)\to(7);\\
(2)\to(3)\to(4)\to(7);\\
(2)\to(5)\to(3)\to(4)\to(7);\\
(2)\to(5)\to(3)\to(7);\\
(2)\to(5)\to(7);\\
(2)\to(3)\to(6)\to(7);\\
(2)\to(3)\to(1);\\
(2)\to(3)\to(4)\to(1);\\
(2)\to(6)\to(3)\to(4)\to(1);\\
(2)\to(6)\to(3)\to(1);\\
(2)\to(5)\to(1);\\
(2)\to(3)\to(6)\to(7).
\end{gathered}
\qquad (8)
$$

6. Після того, як N комп'ютерів було заражено, антивіруси поновлюють власні бази. Це відбувається через деякий час t_m. Тобто через відповідний час вірус гине на всіх машинах, захищених антивірусом – див. табл. 1, п.8. Або можливий інший варіант поновлення – із центрів поновлення засобів захисту у деякий момент часу після виникнення у мережі вірусу починають розповсюджуватись нові антивірусні засоби, які здатні впоратись із даним вірусом. Центр поновлення позначається станом (1), який, по суті аналогічний стану (7) в тому, що зараження вірусом даного типу для нього неможливе. Тоді сусіди центру поновлення переходять до стану (1), і починають розсилати антивіруси далі – див. табл. 1, п.9.

Враховуючи вказані правила та обмеження, приходимо до концепції моделі розповсюдження вірусів як клітинкового автомата, клітинки якого можуть перебувати в станах (1)-(7) та (1а)-(7а), зміни яких відбуваються згідно переходів п 1-9 табл. 1. Однак слід зауважити, що для реального прикладу необов'язково має бути застосована вся сукупність станів та правил переходу, а лише деяка підмножина, що відповідає особливостям заданого типу вірусу. Вважаємо, що початкова картина танів є заданою. Тоді через певний час Δt можемо

одержати картину розподілу заражених комп'ютерів у мережі.

Область застосування запропонованої моделі

Дана модель може бути використана для аналізу розповсюдження шкідливого програмного забезпечення таких видів:

– мережні хробаки;

– класичні комп'ютерні віруси.

Розглянемо відмінність між ними.

Мережні хробаки розповсюджують свої копії в мережі з метою проникнення на віддалені комп'ютери, запуску своєї копії на віддаленому комп'ютері, розповсюдження на інші комп'ютери мережі [3]. Більшість відомих хробаків розповсюджується у вигляді файлів: вкладень у електронний лист, посилань на заражений ресурс тощо. Наприклад, вірус LoveLetter, який розповсюджувався у вигляді замаскованого під текстове вкладення файлу love-letter-for-you.txt.vbs. Для активації користувачеві достатньо було двічі клацнути по даному вкладенню. Деякі види хробаків (так звані пакетні хробаки) розповсюджуються у вигляді мережних пакетів, які проникають безпосередньо у пам'ять комп'ютера та активізують свій код. Хробаки масового розповсюдження, на моделювання яких теж розрахована запропонована модель, сканують книгу адрес та html–файли для одержання списку адрес електронної пошти, а потім розсилають себе за цими адресами (наприклад, Reteras). Інколи адреси задані автором такого хробака (наприклад, Yaha).

Дана модель може ймовірнісно враховувати, що активізація коду мережного хробака відбувається внаслідок таких факторів:

– недоліки в конфігуруванні мережі (наприклад, копіювання на диск, що відкритий на повний доступ);

– помилки в службах безпеки операційної системи.

Людський фактор (запуск шкідливого програмного забезпечення внаслідок вдалого застосування соціального інжинірінгу) в подібному випадку складно врахувати, оскільки імовірності зараження у такому випадку будуть залежати від особливостей поведінки конкретного користувача даного комп'ютера.

Класичні комп'ютерні віруси розповсюджують свої копії по ресурсам локального комп'ютера із метою наступного запуску свого коду при визначених діях користувача чи подальшого розповсюдження в ресурси комп'ютера. На відміну від хробаків, цей вид вірусів не використовує мережні сервіси для проникнення на інші комп'ютери. Спосіб передачі в даному випадку такий: користувач відіслав листа із зараженим вкладенням, вірус інфікував файли на змінному носії, які потім потрапили до іншого комп'ютера і т.і.

В описі запропонованої моделі використано деякі терміни, які з урахуванням вищевказаного будуть мати такий зміст:

1. Комп'ютер заражений – це значить, що вірусу вдалось активізувати свій код (без участі користувача або внаслідок дій користувача).

2. Вірус пересилається далі з даного комп'ютера – якщо моделюється розповсюдження мережного хробака, то це є можливим, якщо список контактів даного комп'ютера непорожній; якщо моделюється розповсюдження мережного хробака із наперед заданим списком адрес – то це можливе, якщо дані комп'ютери існують в цьому списку; якщо моделюється розповсюдження класичного вірусу – це є можливим, якщо файли з даного комп'ютера можуть потрапляти на інші комп'ютери (між ними існує певний безпосередній зв'язок).

3. На комп'ютер потрапив вірус, однак не заразив його – це можливо, якщо користувач не виконав дій, необхідних для зараження, або конфігурація даного комп'ютера виконана таким чином, що унеможливлює активізацію вірусу.

Приклади застосування моделі

Зупинимось детальніше на вірусах класу хробаків. Класичні віруси в теперішній час є менш поширеними, а мережні хробаки набули не лише широкого розповсюдження, але й мають декілька різних видів:

Класичні мережні хробаки – використовують для розповсюдження протоколи мереж. Зазвичай цей тип хробаків розповсюджується із використанням неправильної обробки деякими програмними модулями (зокрема, мережними драйверами) пакетів стеку протоколів tcp/ip.

Поштові хробаки – розповсюджуються електронною поштою.

IRC - хробаки – розповсюджуються по каналам IRC (Internet Relay Chat).

P2P - хробаки – розповсюджуються за допомогою піринговых (peer-to-peer) файлообмінних мереж.

IM - хробаки – використовують для розповсюдження системи миттєвого обміну повідомленнями (IM, Instant Messenger – ICQ, MSN Messenger, AIM та ін.).

Продемонструємо застосування запропонованої моделі на декількох прикладах.

Приклад 1. Представники сімейства Net-Worm.Win32.Sasser використовували вразливість в службі LSASS Microsoft Windows.

Особливості. Зараження відбувається в результаті взаємодії деякого сервера та клієнта (жертви).

Таблиця 2

Схема дії хробака сімейства Net-Worm.Win32.Sasser

Крок атаки	Сервер (джерело зараження)	Клієнт (жертва)
1	Хробак здійснює запуск FTP служби на TCP-порту 5554.	–
2	Обрання IP-адреси для атаки та надсилання запиту на порт 445 по цій адресі, перевіряючи, чи запущена служба LSASS	А) Відповідає на запит – тоді перехід до кроку 3 атаки. Б) Не відповідає на запит – зараження не здійснилось.
3	Надсилає експлойт вразливості служби LSASS на порт, з якого надійшла відповідь	В результаті успішного виконання експлойта запускається командна оболонка на TCP-порту 9996

Через оболонку хробак віддалено виконує завантаження копії хробака по протоколу FTP із запущеного раніше сервера та віддалено активує себе.

Розглянемо, як модифікуються правила формування станів та переходів моделі для цього прикладу.

I – комп'ютер був заражений.

V – на комп'ютер потрапила копія хробака, однак він був блокований АВЗ.

O – на комп'ютері встановлено ОС Windows із визначеною вразливістю LSASS.

A – комп'ютер захищений антивірусним забезпеченням.

A_o – комп'ютер захищений антивірусним забезпеченням, однак воно не діє на даний хробак.

H – хробак був знайдений та знищений.

Ввімкнений комп'ютер може перебувати в одному з 9-ти станів, які характеризуються наступною сукупністю атрибутів:

1. $O \wedge A \wedge \neg I$. Комп'ютер не заражений, оскільки антивірусний захист здатний блокувати втручання хробака.

2. $O \wedge (\neg A \vee A_0) \wedge \neg I$. Комп'ютер не захищений, однак поки що не заражений.

3. $\neg O \wedge \neg I$. Зараження не буде, оскільки тип ОС не задовольняє спеціалізації хробака. Наявність дієздатного антивірусного захисту тут не має значення.

4. $O \wedge I \wedge (\neg A \vee A_o) \wedge R$. Комп'ютер заражений та надсилає хробака далі внаслідок відсутності захисту антивірусними засобами – стан можливий, якщо комп'ютер є джерелом атаки (сервером). Зражений клієнт лише виконує задуми зловмисника, однак не є джерелом розповсюдження хробака.

5. $O \wedge I \wedge (\neg A \vee A_o) \wedge \neg R$. Комп'ютер заражений, однак хробака не надсилає – цей стан типовий для зараженого клієнта.

6. $O \wedge H$. Комп'ютер вилікований.

Можливі такі переходи між станами:

$$2 \rightarrow 5 \rightarrow 6;$$
$$2 \rightarrow 4 \rightarrow 6.$$

Приклад 2. Розглянемо хробаків виду Email-Worm.Win32.Zafi.d.

Особливості. Розповсюджується шляхом розсилання заражених повідомлень-вітань зі святом. Ім'я файлу хробака, який знаходить у вкладенні до листа, – postcard на мові, яка відповідає вітанню, та довільного набору символів. Розширення файлу хробака випадковим чином обирається з наступних: .bat, .com, .exe, .pif, .zip. Для розсилання хробак використовує адреси електронної пошти, знайдені на атакованому комп'ютері. Щоб одержати керування, хробак має бути запущений користувачем.

Таблиця 3

Розповсюдження хробаків виду Email–Worm.Win32.Zafi.d

Джерело зараження	Жертва
Пошук імені жертви в списку розсилки (адреси електронної пошти) та надсилання листа	А) Запуск хробака необережним користувачем. Жертва стає джерелом зараження і розсилає хробака далі. Б) Користувач не активує хробака. Масової розсилки не відбувається, однак можливе ненавмисне відсилання листа із шкідливим вмістом.

Розглянемо, як модифікуються правила формування станів та переходів моделі для цього прикладу. Врахування атрибутів O або $\neg O$, в даному випадку не має змістовного навантаження, оскільки подібні хробаки практично платформонезалежні.

Можна виділити наступні стани:

1. $O \wedge A \wedge \neg I$. Комп'ютер захищений та не заражений.

2. $O \wedge (\neg A \vee A_0) \wedge \neg I$. Комп'ютер не захищений, однак поки що не заражений.

3. $O \wedge I \wedge (\neg A \vee A_0) \wedge R$. Комп'ютер заражений, та надсилає хробака далі внаслідок відсутності захисту антивірусними засобами.

4. $O \wedge (\neg A \vee A_0) \wedge V$. Хробак потрапив на незахищений комп'ютер, однак поки що не активований.

5. $O \wedge A \wedge V$ або $O \wedge A \wedge V \wedge R$ (в разі можливості ненавмисного відсилання листа). Хробак потрапив на захищений комп'ютер, не активований і наступним кроком автоматично буде виявлений та знищений (перехід до стану 6).

6. $O \wedge H$. Комп'ютер вилікований.

Можливі переходи між станами:

$$2 \to 4 \to 3 \to 6 \text{ або } 2 \to 4 \to 3 \to 1;$$
$$1 \to 5 \to 6 \text{ або } 1 \to 5 \to 1.$$

Приклад 3. Розглянемо приклад ІМ-хробака на прикладі IM–Worm.Win32.Kelvir.k

Особливості. ІМ-хробаки рідко надсилають заражені файли безпосередньо між клієнтами. Замість цього вони надсилають посилання на заражені веб-сторінки. Наприклад, хробак надсилає повідомлення, які містять текст типу «ось ваше фото» та посилання, по вказаній у якому адресі розташовано файл хробака.

Таблиця 4

Розповсюдження ІМ-хробака IM-Worm.Win32.Kelvir.k

Джерело зараження	Жертва
Надсилання посилання на заражену веб-сторінку	А) Запуск хробака з віддаленої сторінки необережним користувачем. Б) Користувач не активує хробака.

Модель для цього варіанту буде схожою на модель хробаків Email-Worm.Win32.Zafi.d. Якщо врахувати, що пересилання заражених даних між комп'ютерами фактично не відбувається, то одержуємо таку сукупність станів:

1. $O \wedge A \wedge \neg I$. Комп'ютер захищений, виконання віддаленого зловмисного коду блокується.

2. $O \wedge (\neg A \vee A_0) \wedge \neg I$. Комп'ютер не захищений, однак поки що не заражений.

3. $O \wedge (\neg A \vee A_0) \wedge I$. Комп'ютер не захищений і заражений.

4. $O \wedge (\neg A \vee A_0) \wedge V$. Посилання на хробака потрапило на незахищений комп'ютер, однак поки що не активоване.

5. $O \wedge H$. Комп'ютер вилікований після зараження хробаком.

Переходи між станами здійснюються у такій послідовності:

$$2 \to 4 \to 3 \to 5 \text{ або } 2 \to 4 \to 3 \to 1.$$

Результати обчислювального експерименту

Для ілюстрації принципів дії моделі, представленої співвідношеннями (1)-(7а), (8) було проведено обчислювальний експеримент, візуалізація результатів якого представлена на рис. 1-6. З метою наближення модельної ситуації до реальних умов правила, за якими відбувається (чи не відбувається зараження) прийняті ймовірнісними. При цьому виділено декілька випадків.

Випадок 1. Комп'ютер захищений антивірусом (стани із заданим атрибутом A):

Імовірність зараження $P_{\text{inf}} = k_1$, $k_1 << 1$, імовірність розсилання вірусу $P_{post} = k_2$.

Випадок 2. Комп'ютер не захищений антивірусом (стани із атрибутами $(\neg A \vee A_0)$):

$$P_{\text{inf}} = 1,\ P_{post} = 1.$$

Випадок 3. Якщо у комп'ютера інша операційна система, ніж у зараженого вірусом «сусіда» (стани із атрибутом $(\neg O)$):

$$P_{\text{inf}} = 0,\ P_{post} = k_3.$$

На наведених нижче рисунках кожна клітинка – це комп'ютер, який може перебувати у трьох основних станах:

– не заражений (в цю групу поєднано стани із атрибутом $\neg I$);

– заражений (стани з атрибутами I та V);

– вилікований чи захищений антивірусом (стани з атрибутами A або H).

Базові стани (1)-(7) враховані при написанні програми.

Випадок 4. Поновлення АВЗ відбувається за п.9 (табл. 1).

На рисунках 1-4 світло-сірим кольором позначено комп'ютери, які не є зараженими, темно-сірим – комп'ютери, які на поточний момент інфіковані.

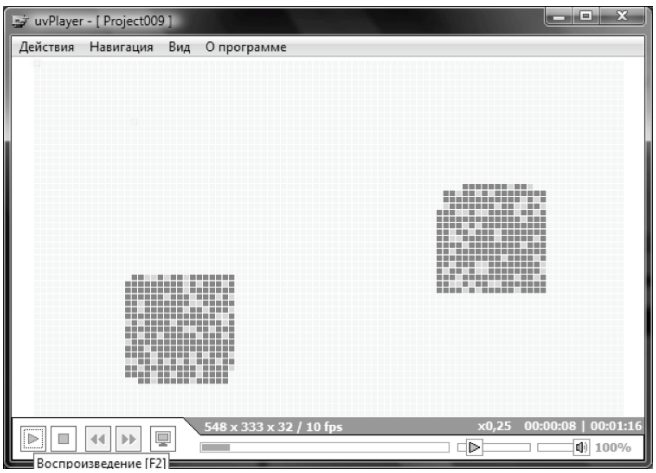

Рис. 1. Розвиток зараження мережі. Довкола джерел зараження (за умовою два джерела) поступово розповсюджується вірус. Джерела зараження інфікують комп'ютери, адреси яких вони «знають». Середньо-сірим кольором в ділянках, яких торкнулось зараження, показуються захищені антивірусом або вилікувані машини (стан (1), (7)).

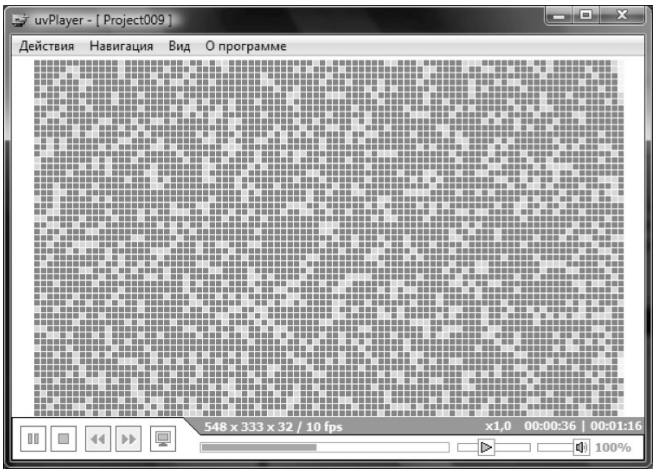

Рис. 2. Зараження досягло піку. Клітинки, зображені більш світлим кольором – комп'ютери, на яких, за умовою, встановлено дієздатні засоби антивірусного захисту.

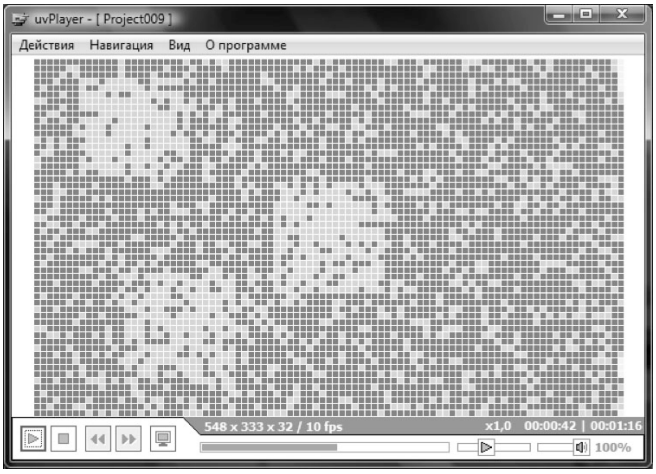

Рис. 3. Навколо центрів поновлення засобів АВЗ комп'ютери починають зцілюватись (ділянки із більш світлим кольором)

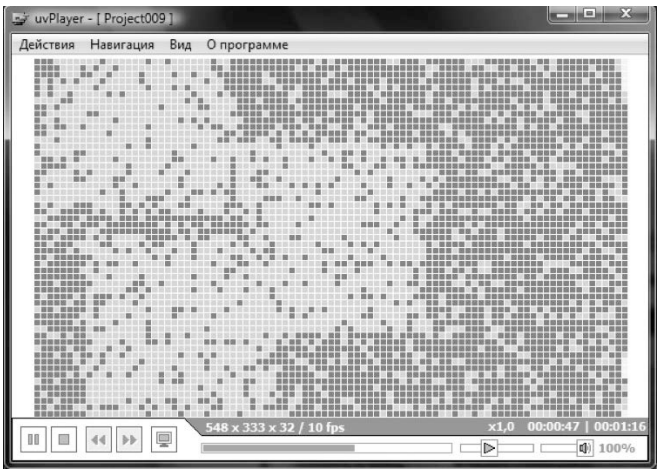

Рис. 4. Розвиток зцілення.

Наприкінці клітинковий автомат приходить до стану, в якому всі увімкнені комп'ютери будуть зцілені (більш світлий колір). Повторне зараження цим самим вірусом неможливе.

Висновки

Запропонована в даній роботі модель та розроблене програмне забезпечення дозволяють прогнозувати ситуацію по інфікуванню мережі. Застосування такої моделі може бути корисним для мереж корпоративного масштабу для вироблення рекомендацій по упередженню зараження найбільш важливих ділянок, визначенню найбільш вразливих місць мережі по відношенню до різних типів вірусів. Ця задача є актуальною, оскільки асортимент шкідливих програм зростає та модифікується швидше, ніж антивірусні засоби. Отже, забезпечити усі станції дієздатним проти усіх вірусів антивірусним забезпеченням не виявляється можливим, а значить, вироблення заходів по своєчасному виявленню та усуненню наслідків дії вірусів, і програмного забезпечення, яке допомагає в цьому процесі, виявляється корисним.

Клітинковий автомат, який відображає стан мережі, в даній роботі прийнятий класичним імовірнісним автоматом із регулярною решіткою, кожна клітинка якого має вісім сусідів для зручності візуалізації результатів роботи. Однак, у разі необхідності, запропонована модель може бути використана для реалізації роботи клітинкового автомату із нерегулярною решіткою будь-якого виду.

ЛІТЕРАТУРА

[1]. Бандман О.Л. Отображение физических процессов на их клеточно–автоматные модели. //Вестник Томского Государственного университета, Управление, вычислительная техника и информатика. – 2008, № 2(3). – С. 6–17.

[2]. Братусь А.С., Новожилов А.С., Платонов А.П. Динамические системы и модели биологии. – ФИЗМАТЛИТ, 2011. – 401 с.

[3]. Грайворонський М.В., Новіков О.М. Безпека інформаційно–комунікаційних систем.–К.: Видавнича група BHV, 2009. – 608 с.
[4]. Котенко И.В., Воронцов В.В. Аналитические модели распространения сетевых червей. – Тр. СПИИРАН, 2007, № 4. – С. 208–224.
[5]. Castillo J.V.R., Navarro B.F., Monteiro L.H.V. Epidemiological models applied to viruses in computer networks //Journal of computer science , No.1 (1), 2005.– pp. 31–34.
[6]. Khan M. S. S. A computer virus propagation model using delay differential equations with probabilistic contagion and immunity // International Journal of Computer Networks & Communications (IJCNC), 2014.– Vol.6, No.5. – pp.111–128.
[7]. Fu S.C., Milne G. Epidemic Modelling Using Cellular Automata [Електронний ресурс].– Режим доступа: http://smr.csse.uwa.edu.au/pdf/EpidemicModellingUsingCA.pdf

REFERENCES

[1]. Bandman O.L. (2008)," Mapping physical processes on their cellular automata models ", Bulletin of Tomsk State University: Control, Computer Science and informatics, No. 2(3), pp. 6–17.
[2]. Bratus A.S., Novozhilov A.S., Platonov A.P. (2011) Dynamic systems and biologic models. Physmatlit, 401 p.
[3]. Graivoronskyi M.V., Novikov O.M. (2009) Information–communication systems security. Kyiv: BHV, 608 p.
[4]. Kotenko I.V., Vorontsov V.V (2007) "Analytical models of network worms propagation", Works of SPIIRAN, No.4., pp. 208–224.
[5]. Castillo J.V.R., Navarro B.F., Monteiro L.H.V (2005) "Epidemiological models applied to viruses in computer networks", Journal of computer science, No.1 (1), pp. 31–34.
[6]. Khan M. S. S. (2014) "A computer virus propagation model using delay differential equations with probabilistic contagion and immunity", International Journal of Computer Networks & Communications (IJCNC), Vol.6, No.5., pp.111–128.
[7]. Fu S.C., Milne G. Epidemic Modelling Using Cellular Automata [Online].– Avaliable from: http://smr.csse.uwa.edu.au/pdf/EpidemicModellingUsingCA.pdf

МОДЕЛИРОВАНИЕ РАСПРОСТРАНЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ НА ОСНОВЕ ВЕРОЯТНОСТНОГО КЛЕТОЧНОГО АВТОМАТА

В условиях возрастания объемов и видов вредоносного программного обеспечения, которое обобщенно называют вирусами, актуальной задачей является моделирование его распространения для принятия упреждающих мероприятий. Существуют модели распространения компьютерных вирусов в виде обыкновенных дифференциальных уравнений, но они не уделяют должного внимания их пространственному распределению и логическим особенностям, сосредотачиваясь на количественных показателях. В данной статье рассмотрен подход к моделированию вирусов на основе клеточного автомата, предложена новая модель распространения вирусов, которая отличается возможностью учитывать некоторые черты самовоспроизводства вредоносного ПО, принимает во внимание действие антивирусной защиты и ее влияние на распространение заражения. Модель применена к ряду практических примеров, в результате моделирования получена информация относительно распределения заражения в сети. Предложенная модель может быть адаптирована к разным видам вредоносного ПО.
Ключевые слова: вредоносное программное обеспечение, вирусы, моделирование, клеточные автоматы.

COMPUTER VIRUSES SIMULATION USING PROBABILISTIC CELLULAR AUTOMATA

In conditions of malware volumes and types growth, which are generally called viruses, the actual problem is simulation of its propagation for taking preventive actions. There are models of computer viruses propagation in form of ordinary differentional equations, but it don't pay appropriate attention to a space distribution and logical peculiarities, concentrating on a quantitative indexes. In the paper the virus modelling approach based on cellular automata is considered. The new model of virus propagation is proposed. The model differs by its possibility to take into account some features of malware replication, antivirus defence and antivirus influence on infection propagation. The model was applied to some practical examples, the information about infection distribution in the network was obtained as a simulation result. The proposed model can be adapted to different types of malware.
Keywords: malware, viruses, simulation, cellular automata.

Грайворонский Николай Владленович, кандидат физико-математических наук, доцент, и.о. заведующего кафедрой информационной безопасности Физико-технического института НТУУ «КПИ».
E–mail: mykola.graivoronskyi@gmail.com
Грайворонський Микола Владленович, кандидат фізико-математичних наук, доцент, в.о. завідувача кафедри інформаційної безпеки Фізико-технічного інституту НТУУ «КПІ».
Grayvoronskyi Mykola, Ph.D., associate professor, head of information security chair in Physics and Technology Institute of NTUU "KPI".

Степочкина Ирина Валериевна, кандидат технических наук, доцент кафедры информационной безопасности Физико-технического института НТУУ «КПИ».
E–mail: Iryna.Styopochkina@gmail.com
Стьопочкіна Ірина Валеріївна, кандидат технічних наук, доцент кафедри інформаційної безпеки Фізико-технічного інституту НТУУ «КПІ».
Styopochkina Iryna, Ph.D., associate professor of information security chair in Physics and Technology Institute of NTUU "KPI"