УДК 004.49.5

Козелков С.В., д.т.н.; **Коршун Н.В.,** к.т.н.; **Браіловський М.М.,** к.т.н.

МАТЕМАТИЧНА МОДЕЛЬ РОЗПОВСЮДЖЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА КОМУТУЮЧИХ ПРИСТРОЯХ ІНФОРМАЦІЙНИХ СИСТЕМ

Kozelkov S.V., Korshun N.V., Brailovskyi M.M. Mathematical model of distribution of harmful software on switching devices of information systems. The preventive methods of warning of introduction and distribution of the harmful programs in the informative systems and control the system are offered. The paper proposes to analysis the permeation of malicious software not only on computers but also on switching devices in information systems. The developed model of finding the mathematical expectation of the number of infected switching devices is based on Markov chain. The author gives a mathematical model of the malicious software spread on the switching devices of information systems. This method allows to define the potential threats of networkof distribution of information and to give the quantitative high-quality estimationof the system durability.

Keywords: Markov chains, mathematical models, switching devices, malicious software, system durability, potential threats

Козелков С.В., Коршун Н.В., Браіловський М.М. Математична модель розповсюдження шкідливого програмного забезпечення на комутуючих пристроях інформаційних систем. У статті запропоновано проводити аналіз впливу шкідливого програмного забезпечення не тільки на комп'ютери, а й на комутаційні пристрої у інформаційних системах. Розроблена модель знаходження математичного очікування кількості заражених комутуючих пристроїв на основі ланцюга Маркова. Запропонована математична модель розповсюдження шкідливого програмного забезпечення на комутуючих пристроях інформаційних систем.

***Ключові слова*:** ланцюги Маркова,математичні моделі, комутуючі пристрої, шкідливе програмне забезпечення, потенціальна загроза

Козелков С.В., Коршун Н.В., Браиловский Н.Н. Математическая модель распространения вредоносного программного обеспечения на коммутирующих устройствах информационных систем. В статье предложено проводить анализ проникновения вредоносного программного обеспечения не только на компьютеры, но и на коммутационные устройства в информационных системах. Разработанная модель нахождения математического ожидания количества зараженных коммутирующих устройств на основе цепи Маркова. Предложена математическая модель распространения вредоносного программного обеспечения на коммутирующих устройствах информационных систем.

Ключевые слова: цепи Маркова, математические модели, коммутирующие устройства, вредоносное программное обеспечение, потенциальная угроза

Постановка задачі. У сучасному суспільстві широкого поширення набули інформаційні мережі, які крім виконання функцій підтримки обміну та отримання інформації та спілкування останнім часом все частіше стають об'єктами і засобами інформаційного управління і ареною інформаційного протиборства [1]. В недалекому майбутньому вони неминуче стануть істотним інструментом інформаційного впливу, в тому числі з метою маніпулювання особистістю, соціальними групами і суспільством в цілому, а також, напевно, полем інформаційних війн [2]. Перехоплення управління мережею давно не новинка, управління і маніпуляція свідомістю – ось актуальні теми сьогодення. У недалекому минулому ми боялися тільки комп'ютерних вірусів, а сьогодні ця небезпека очікується і через інші гаджети (телефони, смартфони, планшети та інше) причому як завдяки дротовим так і безпровідним каналам. На сьогоднішній день комутуючі пристрої мереж теж мають своє програмне забезпечення, тому є можливість впливу шкідливого програмного забезпечення і на ці пристрої. Але, на думку авторів, цій проблемі в наукових дослідженнях не приділяється достатньої уваги.

Тому метою даної статті є створення умов попередження впровадження і поширення шкідливих програм в інформаційних системах, а також системах управління і обміну інформацією. Це можливо робити за допомогою превентивних заходів, таких, як розрахунок

математичного очікування кількості заражених комутуючих пристроїв (КП) в кожному новому сегменті мережі.

Математична модель інформаційної мережі. Розглянемо інформаційну мережу (ІС), що складається з N комутуючих пристроїв. У ній кожен КП може перебувати в одному з двох станів – незаражений або заражений (під «зараженістю» розуміється, що на комутуючий пристрій була здійснена атака, тобто несанкціонований вплив на програмне забезпечення) .

Мережу можна представити у вигляді графа, вузлами якого є КП, а дугами – канали зв'язку між ними, по яким може поширюватися шкідливе програмне забезпечення (ШПЗ) [3]. Вага зв'язку w_{ij} означає ймовірність переходу ШПЗ по каналу зв'язку між i-м та j-м КП за одиницю часу.

При цьому, загальний стан ІС є сукупністю станів всіх КП мережі, яке можна описати вектором з N елементів, де значення i-го елемента відповідає стану i-го КП: I (infected), якщо пристрій заражений; S (suspected), якщо він не заражений.

Стан ІС в наступний момент часу залежить тільки від поточного стану ІС, і не залежить від попередніх. Таким чином, процес поширення ШПЗ в ІС можна уявити як ланцюг Маркова.

Тоді перехідні ймовірності визначаються за формулою:

$$P_{ij} = P\left[f^t = s^j \mid f^{t-1} = s^i \right]. \tag{1}$$

ІС перейде зі стану s_i в стан s_j за умови, якщо кожен КП в ІС перейде зі стану s_k^i в стан s_k^j, де k – номер КП в ІС. Імовірність цієї події описується наступною формулою:

$$P_{ij} = P\left[f^t = s^j \mid f^{t-1} = s^i \right] =$$

$$= P\left[f_1^t = s_1^j \cap f_2^t = s_2^j \cap \ldots \cap f_N^t = f_1^{t-1} = s_1^i \cap f_2^{t-1} = s_2^i \cap \ldots \cap f_N^{t-1} = s_N^i \right] =$$

$$= \prod_{k=1}^{N} P\left[f_k^t = s_k^j \mid f_k^{t-1} = s_k^i \right]. \tag{2}$$

Для визначення ймовірності $P\left[f_k^t = s_k^j \mid f_k^{t-1} = s_k^i \right]$ переходу k-го КП зі стану s_k^i в стан s_k^j необхідно розглянути чотири варіанти для різних станів комутуючого пристрою на попередньому і наступному кроці: перехід зі стану S в стан I, із S в S, із I в S та із I в I.

$S \rightarrow I$. Вірогідність зараження незараженої k-го пристрою при початковому стані ІС s^i дорівнює $P_{зар}(k,s^i)$.

$S \rightarrow S$. Оскільки подія переходу КП в заражений стан і подія, при якому незаражений пристрій залишиться незаражених, утворюють повну групу подій, то ймовірність того, що КП залишиться незараженим буде дорівнює $1–P_{зар}(k,s^i)$.

$I \rightarrow S$. Так як модель не враховує лікування пристрою від ШПЗ, то перехід з стан 1 в стан 0 неможливий, тобто має нульову ймовірність.

$I \rightarrow I$. Так як модель не враховує лікування програмного забезпечення комутатора від ШПЗ, то ймовірність переходу зі стану 1 в стан 1 дорівнює одиниці.

В результаті із врахуванням (1, 2) виходить наступна формула переходів:

$$P\left[f_k^t = s_k^j \mid f_k^{t-1} = s_k^i \right] = \begin{cases} P_{зар}(k,s^i), & z \quad \text{якщо} \quad s_k^i = S, s_k^j = I; \\ 1 - P_{зар}(k,s^i), & \text{якщо} \quad s_k^i = S, s_k^j = S; \\ 0, & \text{якщо} \quad s_k^i = I, s_k^j = S; \\ 1, & \text{якщо} \quad s_k^i = I, s_k^j = I. \end{cases} \tag{3}$$

Вузол k перейде з незараженої стану в заражене за одиницю часу в разі, якщо ШПЗ до нього надійде хоча б з одного іншого вузла (рис. 1).

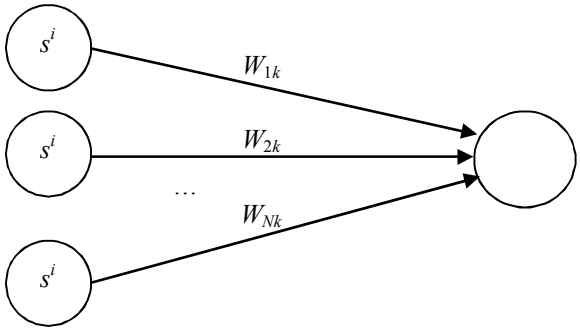

Рис. 1. Схема зараження вузла

Оскільки події зараження *k*-го КП від різних вузлів є незалежними, то ймовірність зараження незараженої *k*-го вузла буде дорівнювати:

$$P_{\text{зар}}\left(k,s^i\right)=1-\prod_{m-1}^{N}\left(1-P_{\text{передачі}}\left(m,k,s_m^i\right)\right). \tag{4}$$

Імовірність передачі ШПЗ від вузла *m* вузлу *k* при стані *m*-го комутатора $s_m{}^i$ можна обчислити таким чином:

– якщо КП *m* заражений, ймовірність дорівнює w_{mk} ;

– якщо КП *m* не заражений, то ймовірність передачі ШПЗ з нього дорівнює нулю.

$$P_{\text{передачі}}\left(m,k,s_m^i\right)=\begin{cases} w_{mk}, & \text{якщо} \quad s_m^i=I \\ 0, & \text{якщо} \quad s_m^i=S \end{cases}; \tag{5}$$

Знайдемо математичне сподівання середнього числа заражених пристроїв на кроці *n*.

Для кожного стану мережі s_j легко визначити кількість заражених КП: оскільки s_j є вектор, що складається з *N* елементів, то кількість заражених КП для стану s_j визначається як

$$N_I\left(s_j\right)=\sum_{i=1}^{N}\begin{cases}1, s_{ij}=I\\0, s_{ij}\neq I\end{cases}.$$

Математичне очікування кількості заражених комутаторів дорівнюватиме:

$$M\left[N_I^t\right]=\sum_{j=1}^{2^N}p_j^{(t)}\cdot N_I\left(s_j\right).$$

Зауважимо: якщо розглядати в вигляді ланцюга Маркова не процес поширення ШПЗ по всій ІС, а побудувати окремий марківський ланцюг для кожного вузла, то це дозволить значно скоротити обсяг обчислень.

У кожен момент часу будь який пристрій з певною ймовірністю може бути як незараженим (*S*), так і зараженим (*I*). Вектор стану в даному випадку складається з двох елементів (в більш загальному може складатися з більшої кількості елементів) – ймовірності того, що пристрій не заражений і ймовірності того, що КП заражений: $p_k^t=\left\{P_k^t(S),P_k^t(I)\right\}$, де *k* – номер КП, *t* – номер кроку.

Враховуючи (3-5) матриця перехідних ймовірностей для даного вузла виглядає наступним чином:

$$P=\begin{pmatrix} P\left(f^t=S\mid f^{t-1}=S\right) & P\left(f^t=I\mid f^{t-1}=S\right)\\ P\left(f^t=S\mid f^{t-1}=I\right) & P\left(f^t=I\mid f^{t-1}=I\right)\end{pmatrix}. \tag{6}$$

Оскільки дана модель не враховує можливість лікування, то перехід зі стану *I* у стан *S* в (6) неможливий, а зі стану *I* можливо потрапити тільки назад в стан *I*, то

$$P\left(f^t=S\mid f^{t-1}=I\right)=0, \qquad P\left(f^t=I\mid f^{t-1}=I\right)=1.$$

Так як сума елементів рядка матриці переходів завжди дорівнює одиниці, то $P\left(f^t = S \mid f^{t-1} = S\right) = 1 - P\left(f^t = I \mid f^{t-1} = S\right)$.

Позначимо $P_{зар}(k) = P\left(f^t = I \mid f^{t-1} = S\right)$, де k – це номер вузла, для якого складається модель. В результаті матриця переходів (6) прийме наступний вигляд:

$$P = \begin{pmatrix} 1 - P_{\text{зар}}(k) & P_{\text{зар}}(k) \\ 0 & 1 \end{pmatrix}, \tag{7}$$

де $P_{\text{зар}}(k)$ – це ймовірність зараження k-го вузла, яка, як було показано вище (4, 5), обчислюється за формулою

$$P_{\text{зар}}(k) = 1 - \prod_{m=1}^{N} \left(1 - P_{\text{передачі}}(m,k)\right). \tag{8}$$

Передача ШПЗ від вузла m вузлу k відбудеться при одночасному настанні таких подій:

– якщо пристрій m заражений на попередньому кроці, ймовірність цієї події дорівнює $P_k^{t-1}(I)$;

– якщо вірус пройде по зв'язку m-k, ймовірність цієї події дорівнює w_{mk}.

Отже, ймовірність передачі ШПЗ від вузла m вузлу k дорівнює добутку ймовірності зараженості комутатора m на попередньому кроці, помноженої на ймовірність переходу ШПЗ по зв'язку m-k:

$$P_{\text{передачі}}(m,k) = P_m^{t-1}(I) \cdot w_{mk}\,. \tag{9}$$

В результаті підстановки (7-9) отримуємо наступну матрицю переходів для окремого вузла:

$$P = \begin{pmatrix} \prod_{m=1}^{N} \left(1 - P_m^{t-1}(I) \cdot w_{mk}\right) & 1 - \prod_{m=1}^{N} \left(1 - P_m^{t-1}(I) \cdot w_{mk}\right) \\ 0 & 1 \end{pmatrix}. \tag{10}$$

Як можна помітити, матриця переходів залежить від стану вузлів ІС на попередньому кроці, отже, ланцюг Маркова для кожного вузла є неоднорідністю.

Для використання моделі на основі ланцюга Маркова необхідно задати початкове розподіл π_0 – вектор ймовірностей знаходження ІС в тому чи іншому стані в початковий момент часу. Вибирається єдине початковий стан мережі f_0, для якого ймовірність приймається рівною одиниці, для інших – нулю:

$$\pi_0 = \left\{p_j^0\right\}, \quad \text{де } p_j^0 = P\left[f_0 = s_j\right] = \begin{cases} 1, f_0 = s_j \\ 0, f_0 \neq s_j \end{cases}.$$

Виходячи з теорії ланцюгів Маркова [4], розподіл на кроці t дорівнюватиме $\pi_t = \pi_{t-1} P$.

Початковий розподіл задається для кожного вузла мережі: $\pi_j^0 = \left\{P_j^0(S), P_j^0(I)\right\}$, де j – номер вузла. Найзручніше вибрати в ІС заражені пристрої, для яких ймовірність знаходження в зараженому стані дорівнює 1, тобто $\pi_j^0 = \{0;1\}$, а для інших – навпаки $\pi_j^0 = \{1;0\}$.

Далі для кожного кроку t застосовується наступний алгоритм:

– для кожного j-го вузла за формулою (10) будується матриця переходів;

– вектор початкового на попередньому кроці множиться на отриману матрицю переходів, в результаті виходить вектор розподілу для першого кроку: $\pi_j^t = \pi_j^{t-1} P$;

– маючи множину векторів розподілу на кроці t дорівнює $\left\{\pi_1^t, \pi_2^t, \ldots, \pi_N^t\right\}$, а отже, знаючи ймовірність знаходження кожного вузла в зараженому стані в момент часу t $\left(P_j^t(I)\right)$,

можна обчислити математичне очікування кількості заражених комутуючих пристроїв на цьому кроці: $M\left[N_I^t\right]=\sum_{j=1}^{N} P_j^t(I).$

Приклад роботи запропонованої моделі. Складемо схему з міністанів елементів вузла ІС переходу з незараженого стану в заражений, взявши комутуючий пристрій, пов'язаний каналами зв'язку, за якими може поширюватися ШПЗ з іншими пристроями (рис. 2):

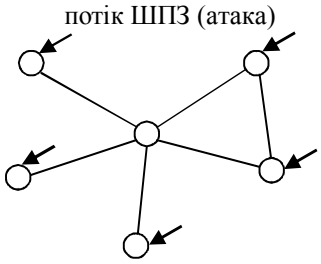

Рис. 2. Вузол ІС

Введемо позначення:

$p_з$ – ймовірність зараження;

$p_a = \mu \cdot t$ – пуассонівський потік атак на елементи вузла;

$p_к = p_з \cdot \left[1 - \sum_{i \text{ по перестановках}} \prod_{j=1}^{k} \left(1 - p_{ij}\right)\right]$ – імовірність переходу з незараженого стану в заражений.

Тоді схема переходів станів елементів ІС буде виглядати наступним чином (рис. 3).

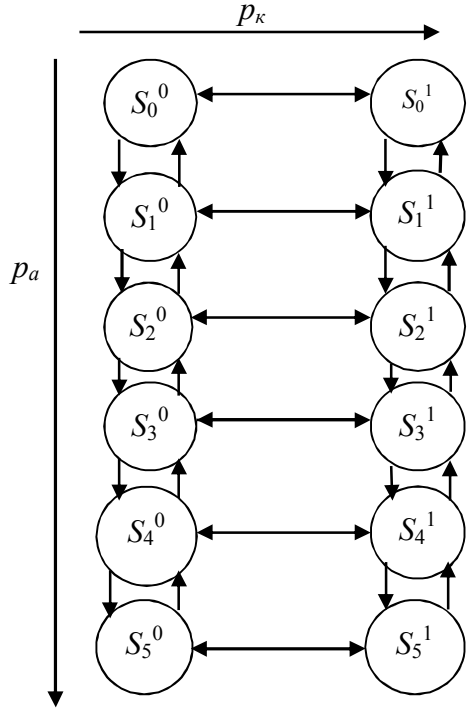

Рис. 3. Схема зміни станів елементів вузла ІС

На основі схеми зміни станів елементів вузла ІС побудуємо ймовірнісну схему зв'язків у вигляді стохастичної матриці:

	S_0^0	S_0^1	S_1^0	S_1^1	S_2^0	S_2^1	S_3^0	S_3^1	S_4^0	S_4^1	S_5^0	S_5^1
S_0^0	$1-p_a$	*0*	*0*	0	0	0	0	0	0	0	0	0
S_0^1	0	$1-p_a$	0	*0*	0	0	0	0	0	0	0	0
S_1^0	p_a	0	$1-p_a-p_к$	*0*	0	0	0	0	0	0	0	0
S_1^1	0	p_a	$p_к$	$1-p_a$	0	0	0	0	0	0	0	0
S_2^0	0	0	p_a	0	$1-p_a-p_к$	*0*	0	0	0	0	0	0
S_2^1	0	0	0	p_a	$p_к$	$1-p_a$	0	0	0	0	0	0
S_3^0	0	0	0	0	p_a	0	$1-p_a-p_к$	*0*	0	0	0	0
S_3^1	0	0	0	0	0	p_a	$p_к$	$1-p_a$	0	0	0	0
S_4^0	0	0	0	0	0	0	p_a	0	$1-p_a-p_к$	*0*	0	0
S_4^1	0	0	0	0	0	0	0	p_a	$p_к$	$1-p_a$	0	0
S_5^0	0	0	0	0	0	0	0	0	p_a	0	$1-p_к$	*0*
S_5^1	0	0	0	0	0	0	0	0	0	p_a	$p_к$	10

Висновки. Таким чином, дана методика дозволяє визначити потенційні загрози мережі поширення інформації, а також дати кількісну, а потім якісну оцінку життєстійкості системи. Пропонується розглядати у вигляді ланцюга Маркова не процес поширення ШПЗ по всій ІС, а будувати окремий марківський ланцюг для кожного вузла, що дозволить значно скоротити обсяг обчислень і енерговитрат. Контроль на вході кожного з сегментів мережі дозволить швидко приймати необхідні дії по недопущенню розповсюдження ШПЗ.

Література

1. Управління передачею даних в інфокомунікаційних мережах : навч. посібник / С.В. Козелков, К.С. Козелкова. – Київ: ДУТ, 2014. – 345 с.

2. Браиловский Н.Н. Модели управления в системах обеспечения информационной безопасности государства / Н.Н. Браиловский, С.В. Зыбин, В.А. Хорошко // Інформатика та математичні методи в моделюванні. – 2014. –Т.4. – № 4. – С. 304-311.

3. Бойченко О.В. Модель корпоративного інформаційного захисту об'єкту інформатизації / О.В. Бойченко, Я.І. Торошанко // Наукові записки Українського науково-дослідного інституту зв'язку. – 2011. – №4(20). – С. 15-19.

4. Нуммелин Э. Общие неприводимые цепи Маркова и неотрицательные операторы / Э. Нуммелин. – Москва : Мир, 1989. – 207 с.

Автори статті

Козелков Сергій Вікторович – доктор технічних наук, професор, директор Навчально-наукового інституту телекомунікацій та інформатизації, Державний університет телекомунікацій, Київ. Тел.: +380 (96) 017 31 80. E-mail: S.Kozelkov@dut.edu.ua

Коршун Наталія Володимирівна – кандидат технічних наук, декан факультету телекомунікацій, Державний університет телекомунікацій, Київ. Тел. +380 (93) 603 90 64. E-mail: natalie_korshun@ukr.net.

Браіловський Микола Миколайович – кандидат технічних наук, завідувач кафедри системного аналізу, Державний університет телекомунікацій, Київ. Тел.: +380 (67) 429 20 56. E-mail: kcm_dut@ukr.net).

Authors of the article

Kozelkov Serhiy Viktorovych – doctor of sciences (technical), director of the Educational-scientific Institute of the telecommunications and informatization, State University of Telecommunications, Kyiv. Tel.: +380 (96) 017 31 80. E-mail: S.Kozelkov@dut.edu.ua

Korshun Nataliya Volodymyrivna – candidate of sciences (technical), dean of telecommunications faculty, State University of Telecommunications, Kyiv. Tel.: +380 (93) 603 90 64. E-mail: natalie_korshun@ukr.net.

Brailovskyy Mykola Mykolayovych – candidate of sciences (technical), head of systems analysis department, State University of Telecommunications, Kyiv. Tel.: +380 (67) 429 20 56. E-mail: kcm_dut@ukr.net).

Дата надходження в редакцію: 7.03.2016 р. Рецензент: д.т.н., проф. Л.Н. Беркман