ISSN: 2219-8229
E-ISSN: 2224-0136
Founder: Academic Publishing House *Researcher*
DOI: 10.13187/issn.2219-8229
Has been issued since 2010.

European Researcher. International Multidisciplinary Journal

UDC 004.49.5

A Mathematical Model for Technology for Spreading Malicious Software across Heterogeneous Networks based on Markov Chains

[1] Sergey G. Semenov
[2] Vyacheslav V. Davydov

[1] National Technical University "Kharkov Polytechnic Institute", Ukraine
Frunze street 21, Kharkov, 61000
PhD (technical), Assistant Professor
E-mail: s_semenov@ukr.net
[2] National Technical University "Kharkov Polytechnic Institute", Ukraine
Frunze street 21, Kharkov, 61000
Teacher
E-mail: davs87@inbox.ru

Abstract. This article examines existing techniques in mathematical modeling of technology for spreading malicious software across heterogeneous computer networks. The author makes a conclusion about the expediency of using the PSIDR and PSIDDR technology for new solutions. The author employs the graph technique (Markov chains) as the primary technique for mathematical modeling. Based on Markov chains, the author develops mathematical models for spreading computer viruses across heterogeneous computer networks, which are inclusive of its topological, architectural, and functional characteristics. The author has conducted comparative studies into the developed mathematical models and constructed comparative graphs for the dependency of the number of affected nodes on the functioning time of the computer system at the time the virus is being spread. The author makes a conclusion about the expediency of using the developed models in designing heterogeneous computer networks. Bibliography.: 8 items; figures: 4.

Keywords: mathematical model; malicious software; heterogeneous computer network; Markov chains.

Введение. На современном этапе развития компьютерных систем и систем актуальным остается вопрос оптимизации использования существующих телекоммуникационных ресурсов, аппаратных и программных средств. Особенно острой данная проблематика выглядит в условиях внешних воздействий злоумышленного программного обеспечения. При этом решение данной задачи невозможно без предварительного моеделирования возможных неблагоприятных ситуаций и угроз.

В работах [1-4] был описан биологический подход математического моделирования распространения программных угроз (SIT, SIRT, PSIDRT, PSIDDR). Анализ проведенных исследований показал их преимущества (простота использования, низкое время моделирования, использование минимум входных данных) и недостатки (математические модели не учитывают особенности структурного и функционального построения сети, имеют низкую точность в условиях топологических изменений в построении гетерогенных компьютерных сетей и др.).

Анализ литературы известных **материалов и методов** [5, 6] показал, что устранение указанных недостатков возможно путем разработки и построения математической модели на основе цепей Маркова [7].

Целесообразность данного подхода математического моделирования обусловлена тем, что сравнительно небольшое число входящих в марковскую модель параметров обеспечивает относительную простоту ее применения по сравнению, например, с динамическими моделями [8]. Кроме того, в рассматриваемых в математической модели распространения злоумышленного программного обеспечения процессах существует ряд особенностей. В частности это возможные случайные отклонения от заданных режимов работы и взаимосвязь (взаимозависимость) переменных состояния систем во времени.

Данные особенности так же учитываются при математическом моделировании технологии распространения программных угроз с помощью цепей Маркова.

Основная часть

Обсуждения. Рассмотрим локальную сеть, состоящую из N компьютеров. Каждый компьютер может находиться в одном из нескольких состояний, согласно выбранной модели (PSIDR [1, 2], PSIDDR [3]).

Сеть можно представить в виде графа, узлами которого являются компьютеры, а дугами – каналы связи между ними, по которым может распространяться злоумышленное программное обеспечение. Вес связи w_{ij} означает вероятность перехода злоумышленного программного обеспечения по каналу связи между компьютерами i и j за единицу времени.

В постановке задачи моделирования следует отметить, что общее состояние сети в момент времени t является совокупностью состояний всех узлов сети. Оно может быть описано вектором из N элементов, где значение k-го элемента соответствует состоянию k-го узла.

Состояние компьютерной сети в следующий момент времени зависит только от текущего состояния сети и не зависит от предыдущих. Следовательно, процесс распространения злоумышленного программного обеспечения в сети можно представить в виде цепи Маркова [5, 6, 7].

Переходные вероятности вычисляются по формуле:

$$P_{ij} = P\left(f^{(t)} = s^{(j)} \middle| f^{(t-1)} = s^{(i)} \right), \quad (1)$$

где s – состояние узла связи.

Компьютерная сеть перейдет из состояния s_i в состояние s_j при условии, что если каждый узел сети перейдет из состояния $s_k^{(i)}$ в состояние $s_k^{(j)}$, где k – номер узла в компьютерной сети. Вероятность этого события описывается следующей формулой:

$$\begin{aligned} P_{ij} &= P\left(f^{(t)} = s^{(j)} \middle| f^{(t-1)} = s^{(i)} \right) = \\ &= P\left(\begin{array}{l} f_1^{(t)} = s_1^{(j)} \cap f_2^{(t)} = s_2^{(j)} \cap \ldots \cap f_N^{(t)} = f_1^{(t-1)} = \\ = s_1^{(j)} \cap f_2^{(t-1)} = s_2^{(i)} \cap \ldots \cap f_N^{(t-1)} = s_N^{(i)} \end{array} \right) = \\ &= \prod_{k=1}^{N} P\left(f_k^{(t)} = s_k^{(j)} \middle| f_k^{(t-1)} = s_k^{(i)} \right). \end{aligned} \quad (2)$$

Для определения вероятности $P\left(f_k^{(t)} = s_k^{(j)} \middle| f_k^{(t-1)} = s_k^{(i)} \right)$ перехода k-го компьютера из состояния $s_k^{(i)}$ в состояние $s_k^{(j)}$ в математических моделях распространения злоумышленного программного обеспечения необходимо рассмотреть

множество V вариантов для различных состояний компьютера на предыдущем и текущем шаге. Для каждого вида математического моделирования это множество будет различно.

Вероятность передачи злоумышленного программного обеспечения от узла m узлу k при состоянии сети $s_m^{(i)}$ можно вычислить следующим образом: если компьютер m заражен, вероятность равна $p_{пер}^{(m,k)}$, а если компьютер m не заражен, то вероятность передачи злоумышленного программного обеспечения от него равна нулю:

$$P_{пер}^{(m,k,s_m^{(i)})} = \begin{cases} p_{пер}^{(m,k)}, если\ s_m^{(i)} = I, \\ 0, если\ s_m^{(i)} = S. \end{cases} \quad (3)$$

Узел k перейдет из незараженного состояния в зараженное за единицу времени в том случае, если злоумышленное программное обеспечение к нему проникло, хотя бы с одного другого узла.

Рассмотрим более подробно математические модели PSIDR и PSIDDR.

Алгоритм распространения злоумышленного программного обеспечения в соответствии с моделью PSIDR с учетом цепей Маркова (PSIDRM).

Рассматривая модель PSIDR [1, 2], и выделить шестнадцать $V = \{v_1, v_2, \ldots, v_{16}\}$ вариантов различных состояний компьютера:

S → I. Вероятность заражения незараженного k-го компьютера в исходном состоянии компьютерной сети $s^{(i)}$ равна $P_{зар}^{(k,s^{(i)})}$.

S → D. Вероятность детектирования незараженого объекта в соответствии с начальными условиями моделирования PSIDR равна нулю.

S → R. Вероятность подобного перехода (иммунизация незараженного k-го компьютера в исходном состоянии компьютерной сети $s^{(i)}$) равна вероятности иммунизации $P_{им}^{(k,s^{(i)})}$, так как начальными условиями моделирования предусмотрена возможность процесса иммунизации незараженного компьютера.

S → S. Вероятность того, что узел останется в первоначальном состоянии, равна $1 - P_{зар}^{(k,s^{(i)})} - P_{им}^{(k,s^{(i)})}$, так как переходы компьютера из состояния S в состояния I, R и D образуют полную группу событий.

I → S. Вероятность подобного восстановления компьютера в рассматриваемой модели равна нулю, так как начальными условиями моделирования процесс лечения без процессов детектирования и иммунизации (без учета состояний и R) не предусмотрен.

I → R. Вероятность лечения и иммунизации зараженного компьютера равна нулю, так как начальными условиями моделирования процесс лечения и иммунизации без предварительного детектирования не предусмотрен..

I → D. Вероятность детектирования зараженного k-го компьютера в некотором исходном состоянии компьютерной сети $s^{(i)}$ равна $P_{дет}^{(k,s^{(i)})}$.

I → I. Вероятность того, что компьютер останется зараженным, равна $1 - P_{дет}^{(k,s^{(i)})}$, так как переходы компьютера из состояния I в состояния I, R, S и D образуют полную группу событий.

D → S. Вероятность подобного восстановления компьютера в рассматриваемой модели PSIDR равна нулю (исходя из начальных условий моделирования).

D → I. Аналогично предыдущему примеру вероятность подобного восстановления компьютера в рассматриваемой модели PSIDR равна нулю.

D → R. Вероятность лечения зараженного k-го компьютера в некотором состоянии компьютерной сети s(i) равна $P_{леч}^{(k,s^{(i)})}$

D → D. Вероятность того, что компьютер останется в состоянии D, равна $1-P_{леч}^{(k,s^{(i)})}$, так как переход компьютера из состояния D в состояния S, I, и R образуют полную группу событий.

R → S. Вероятность подобного перехода равна нулю, в связи с поставленными начальными ограничениями (иммунизированный узел конечная точка модели).

R → I. Вероятность того, что компьютер будет заражен заново, равна нулю, так как начальными условиями моделирования PSIDR процесс заражения компьютера, обладающего иммунитетом, не предусмотрен.

R → D. Вероятность подобного перехода равна нулю, в связи с поставленными начальными ограничениями.

R → R. Вероятность подобного перехода равна единице, в связи с поставленными начальными ограничениями.

Процесс распространения злоумышленного программного обеспечения в соответствии с моделью PSIDR может быть описан с помощью системы:

$$P\left(f_k^{(t)}=s_k^{(j)}\middle|\, f_k^{(t-1)}=s_k^{(i)}\right)=\begin{cases} P_{зар}^{(k,s^{(i)})}, если\ s_k^{(i)}=S, s_k^{(j)}=I, \\ 1-P_{зар}^{(k,s^{(i)})}, если\ s_k^{(i)}=S, s_k^{(j)}=S, \\ 1-P_{зар}^{(k,s^{(i)})}-P_{им}^{(k,s^{(i)})}, если\ s_k^{(i)}=S, s_k^{(j)}=R, \\ 0, если\ s_k^{(i)}=S, s_k^{(j)}=D, \\ 1-P_{дет}^{(k,s^{(i)})}, если\ s_k^{(i)}=I, s_k^{(j)}=I, \\ 0, если\ s_k^{(i)}=I, s_k^{(j)}\in\{S,R\}, \\ P_{дет}^{(k,s^{(i)})}, если\ s_k^{(i)}=I, s_k^{(j)}=D, \\ 0, если\ s_k^{(i)}=D, s_k^{(j)}\in\{I,S\}, \\ P_{леч}^{(k,s^{(i)})}, если\ s_k^{(i)}=D, s_k^{(j)}=R, \\ 1-P_{леч}^{(k,s^{(i)})}, если\ s_k^{(i)}=D, s_k^{(j)}=D, \\ 0, если\ s_k^{(i)}=R, s_k^{(j)}\in\{I,S,D\}, \\ 1, если\ s_k^{(i)}=R, s_k^{(j)}=R. \end{cases} \quad (4)$$

Поскольку события заражения i-го узла от различных источников являются независимыми, то:

1) вероятность заражения незараженного i-го узла описывается выражением

$$P_{зар}^{(k,s^{(i)})}=1-\prod_{m=1}^{N}\left(1-P_{пер}^{(m,k,s_m^{(i)})}\right). \quad (5)$$

2) вероятность восстановления зараженного i-го узла описывается выражением

$$R_i=1-(1-R_i)\cdot(1-RECOVER_{coeff}), \quad (6)$$

где R_i – коэффициент восстановления i-го узла, $RECOVER_{coeff}$ – вероятность вылечивания узла.

3) вероятность детектирования зараженного i-го узла описывается выражением:

$$D_i = 1 - \left(1 - D_i\right) \cdot \left(DETECTION_i \left[OS\_TYPE \right] \right), \quad (7)$$

где D_i – коэффициент детектирования i-го узла,

$DETECTION_i \left[OS\_TYPE \right]$ – уровень детектирования i-го узла в зависимости от типа операционной системы.

Алгоритм распространения злоумышленного программного обеспечения в соответствии с моделью PSIDDR с учетом цепей Маркова (PSIDDRM).

Аналогичным образом можно рассмотреть модель PSIDDR, и выделить двадцать пять $V = \{v_1, v_2, \ldots, v_{25}\}$ вариантов различных состояний компьютера, при этом 16 вариантов (переходы между состояниями {S, I, R, D} идентичны переходам из модели PSIDR):

S → X. Вероятность подобного перехода равна нулю, в связи с поставленными начальными ограничениями (незараженный узел не может быть выведен из строя).

I → *I*. Вероятность того, что компьютер останется зараженным, равна $1 - P_{дет}^{(k,s^{(i)})} - P_{вис}^{(k,s^{(i)})}$.

D → *D*. Вероятность того, что компьютер останется в состоянии *D*, равна $1 - P_{леч}^{(k,s^{(i)})} - P_{вис}^{(k,s^{(i)})}$.

I → X. Вероятность выведения k-ого узла из строя равна $P_{вис}^{(k,s^{(i)})}$.

D → X. Вероятность выведения k-ого узла из строя равна $P_{вис}^{(k,s^{(i)})}$.

R → X. Вероятность подобного перехода равна нулю, в связи с поставленными начальными ограничениями (незараженный узел не может быть выведен из строя)

X → S. Вероятность подобного перехода равна нулю, в связи с поставленными начальными ограничениями (состояние «выведенный из строя» - конечное состояние объекта).

X → I. Вероятность подобного перехода равна нулю, в связи с поставленными начальными ограничениями (состояние «выведенный из строя» - конечное состояние объекта).

X → D. Вероятность подобного перехода равна нулю, в связи с поставленными начальными ограничениями (состояние «выведенный из строя» - конечное состояние объекта).

X → R. Вероятность подобного перехода равна нулю, в связи с поставленными начальными ограничениями (состояние «выведенный из строя» - конечное состояние объекта)

X → X. Вероятность подобного перехода равна единице, в связи с поставленными начальными ограничениями.

Процесс распространения злоумышленного программного обеспечения в соответствии с моделью PSIDDR может быть описан с помощью системы (9).

Поскольку события заражения i-го узла от различных источников являются независимыми, то:

1) вероятность заражения незараженного i-го узла описывается выражением (5)
2) вероятность восстановления зараженного i-го узла описывается выражением (6)
3) вероятность детектирования зараженного i-го узла описывается выражением (7)

4) вероятность выхода из строя зараженного/детектированного i-го узла описывается выражением:

$$X_i = 1-(1-X_i)\cdot(1-DEATH_{coeff}), \quad (8)$$

где X_i – коэффициент детектирования i-го узла,

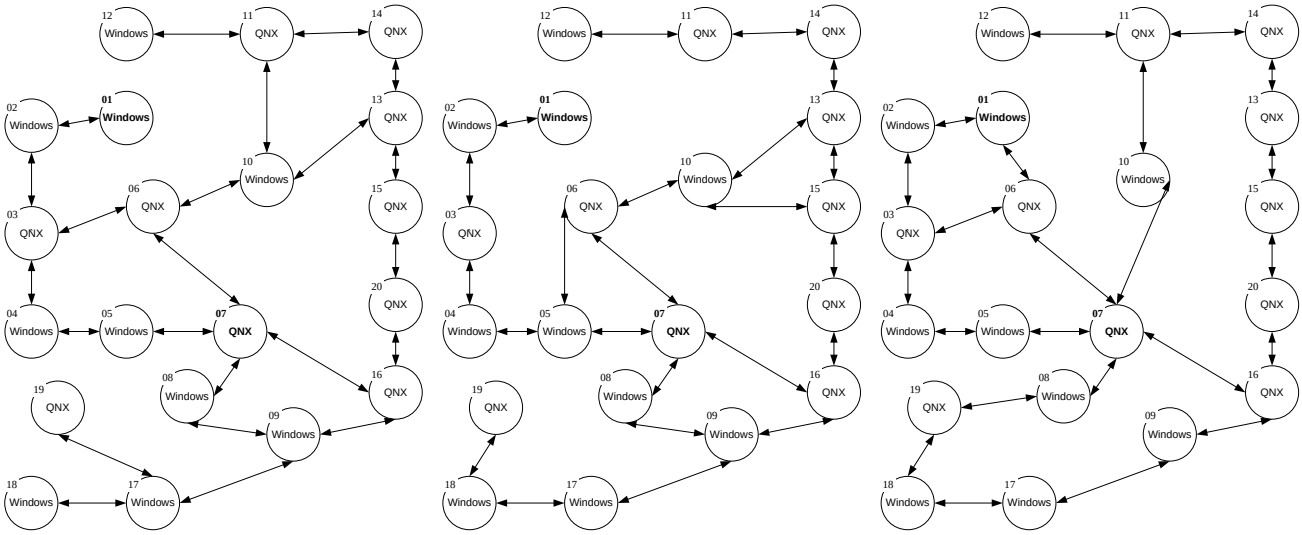
$DEATH_{coeff}$ – уровень выхода из строя i-го.

$$P\left(f_k^{(t)} = s_k^{(j)} \middle| f_k^{(t-1)} = s_k^{(i)}\right) = \begin{cases} P_{зар}^{(k,s^{(i)})}, \text{если } s_k^{(i)} = S,\ s_k^{(j)} = I, \\ 1-P_{зар}^{(k,s^{(i)})}, \text{если } s_k^{(i)} = S,\ s_k^{(j)} = S, \\ 1-P_{зар}^{(k,s^{(i)})} - P_{им}^{(k,s^{(i)})}, \text{если } s_k^{(i)} = S,\ s_k^{(j)} = R, \\ 0, \text{если } s_k^{(i)} = S,\ s_k^{(j)} = D, \\ 1-P_{дет}^{(k,s^{(i)})} - P_{вис}^{(k,s^{(i)})}, \text{если } s_k^{(i)} = I,\ s_k^{(j)} = I, \\ 0, \text{если } s_k^{(i)} = I,\ s_k^{(j)} \in \{S,R\}, \\ P_{дет}^{(k,s^{(i)})}, \text{если } s_k^{(i)} = I,\ s_k^{(j)} = D, \\ 0, \text{если } s_k^{(i)} = D,\ s_k^{(j)} \in \{I,S\}, \\ P_{леч}^{(k,s^{(i)})}, \text{если } s_k^{(i)} = D,\ s_k^{(j)} = R, \\ 1-P_{леч}^{(k,s^{(i)})} - P_{вис}^{(k,s^{(i)})}, \text{если } s_k^{(i)} = D,\ s_k^{(j)} = D, \\ 0, \text{если } s_k^{(i)} = R,\ s_k^{(j)} \in \{I,S,D\}, \\ 0, \text{если } s_k^{(i)} = X,\ s_k^{(j)} \in \{R,I,S,D\}, \\ 1, \text{если } s_k^{(i)} = X,\ s_k^{(j)} = X, \\ 0, \text{если } s_k^{(i)} \in \{S,R\},\ s_k^{(j)} = X, \\ P_{вис}, \text{если } s_k^{(i)} \in \{\mathrm{I},\mathrm{D}\},\ s_k^{(j)} = X, \\ 1, \text{если } s_k^{(i)} = R,\ s_k^{(j)} = R. \end{cases} \quad (9)$$

Оценка результатов исследования. Проведем моделирование разработанных алгоритмов на основе цепей Маркова.

При моделировании распространения злоумышленного ПО на основе алгоритмов PSIDRM и PSIDDRM использовалась топологии, представленные на рис. 1.

Представлены на рис. 1 топологии сетей состоят из 20 узлов. Каждый узел имеет свою операционную систему (QNX или Windows). В зависимости от типа ОС на узле, в процессе моделирования варьируются коэффициенты заражения, лечения и детерминации программной угрозы для данного узла. Топологии отличаются между собой типом связности между узлами. Так, топология, изображенная на рис. 1.а отличается от топологии, изображенной на рис. 1.б наличием разреженности связности по краям, при этом общий коэффициент связности остался тот же.



а) б) в)

Рис. 1. Топологии, используемые при моделировании PSIDRM и PSIDDRM

На рис. 2 представлены кривые распространения программных угроз в гетерогенных компьютерных сетях при использовании алгоритма PSIDRM. При моделировании варьировался коэффициент заражения системы, при котором флаг состояния переходит в положение «зараженный», и в соответствии с алгоритмом распространения злоумышленного программного обеспечения PSIDRM начинается выполнение второго этапа (детектирования и лечения). Анализ кривых рис. 2 показал, что чем ниже данное значение, тем быстрее происходит восстановление системы.

На рис. 3 представлены кривые распространения программных угроз на основе модели PSIDRM в гетерогенных компьютерных сетях, описанных топологиями, представленными на рис. 1. Анализ кривых рис. 3 показал, что наличие разреженных участков увеличивает время заражения системы, при этом может затянуться лечение узлов, находящихся в угловых участках сети.

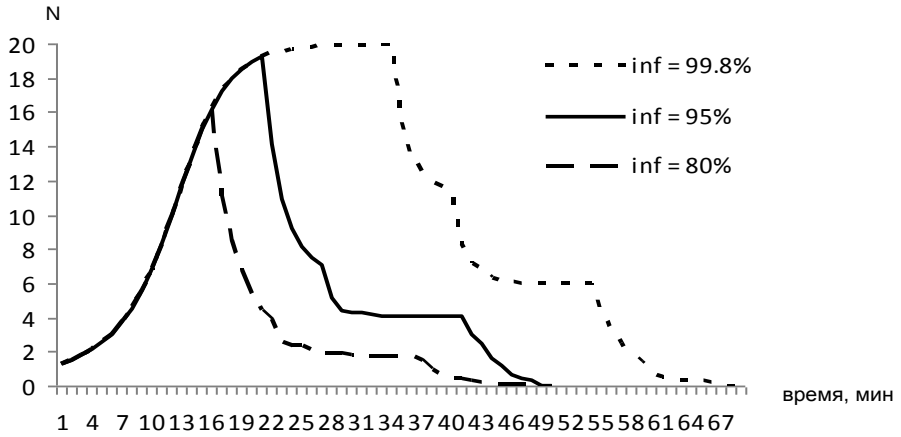


Рис. 2. Кривые зависимости распространения программных угроз от времени, используя алгоритм PSIDRM при различных коэффициентах заражения «LIMIT_SYSTEM_DETECTED_AS_INFECTED»

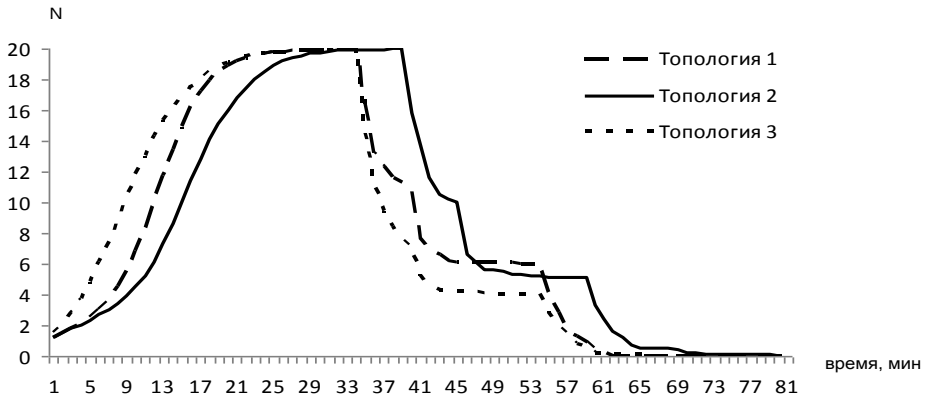


Рис. 3. Кривые зависимости количества зараженных от времени в различных гетерогенных компьютерных сетях на основе алгоритма PSIDRM

На рис. 4 представлены сравнительные кривые распространения программных угроз в гетерогенной компьютерной сети с топологией, изображенной на рис 1.а. Анализ кривых рис. 4 показал, что в при коэффициенте выхода из строя = 1 %, по алгоритму PDIDDRM после вылечивания системы остаются 2 выведенных из строя узла.

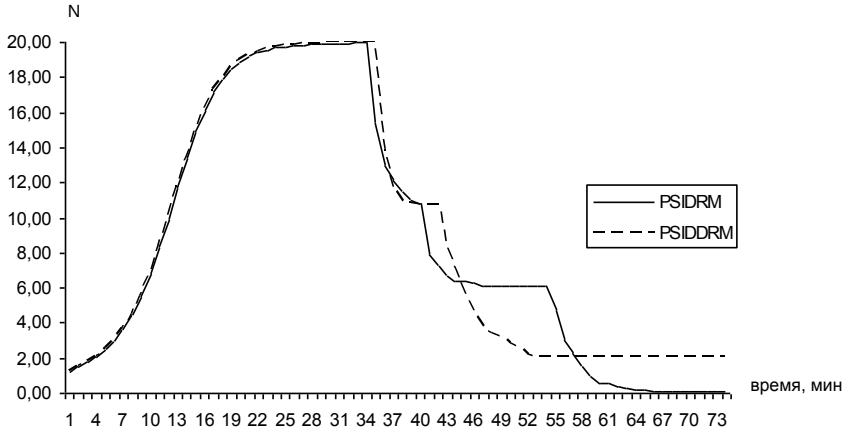


Рис. 4. Кривые зависимости количества зараженных от времени в различных гетерогенных компьютерных сетях (топология 1 (рис. 1.а)) на основе алгоритмов PSIDRM и PSIDDRM

Заключение. В результате проведенной работы была разработана математическая модель (PSIDDRM) распространения злоумышленного программного обеспечения в гетерогенных компьютерных сетях с учетом их топологических и функциональных особенностей на основе цепей Маркова.

Проведенные исследования показали, что использование разработанной модели PSIDDRM позволит до 10% повысить точность оценки количества выведенных из строя узлов по завершению этапа лечения системы. Оценка проведенных исследований позволила сделать вывод о целесообразности применения разработанной модели при проектировании гетерогенных компьютерных сетей.

Примечания:

1. Давыдов В.В. Сравнительный анализ моделей распространения компьютерных вирусов в автоматизированных системах управления технологическим процессом / В.В. Давыдов // Системи обробки інформації. Харків: ХУПС, 2012. Вип. 3(101), Том 2. С. 147-151.

2. Семенов С.Г., Давыдов В.В. Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом / С.Г. Семенов, В.В. Давыдов // Вестник НТУ

«ХПИ». Сборник научных трудов. Серия: Информатика и поделирование. Харьков: НТУ «ХПИ», 2012. №38. С. 163-171.

3. Семенов С.Г., Давыдов В.В. Математическая модель технологии распространения злоумышленного программного обеспечения в компьютерных сетях / С.Г. Семенов, В.В. Давыдов // Восточно-европейский журнал передовых технологий. Харьков, 2013. Вып. 1/4 (61). С. 11-14.

4. M.M. Williamson, J. Leveille Epidemiological model of virus spread and cleanup. HPL-2003-39 [Электронный ресурс. – Режим доступа: http://www.hpl.hp.com/techreports /2003/HPL-2003-39.pdf (дата обращения: 08.01.14)

5. Бабанин, Д.В. Модели распространения компьютерных вирусов на основе цепей Маркова / Д.В. Бабанин // Математическое и программное обеспечение вычислительных систем: межвуз. сб. науч. тр. / под ред. А.Н. Пылькина. М.: Горячая линия - Телеком, 2009. 156 с. С. 89-93.

6. Бабанин Д.В. Оценка структурной защищенности компьютерной сети от вирусных атак / Д.В. Бабанин // Математическое и программное обеспечение вычислительных систем: межвуз. сб. науч. тр. / Под ред. А.Н. Пылькина — Рязань: РГРТУ, 2011. 224 с. С. 133-138.

7. Кемени Дж. Дж. Конечные цепи Маркова / Дж. Дж. Кемени, Дж. Л. Снелл. М.: Наука. 1970. 272 с.

8. Малинецкий Г.Г. Нелинейная динамика: подходы, результаты, надежды / Г.Г. Малинецкий, А.Б. Потапов, А.В. Подлазов. М.: УРСС, 2006.

References:

1. Davydov V.V. Sravnitel'nyi analiz modelei rasprostraneniya komp'yuternykh virusov v avtomatizirovannykh sistemakh upravleniya tekhnologicheskim protsessom / V.V. Davydov // Sictemi obrobki informatsiї. Kharkiv: KhUPS, 2012. Vip. 3(101), Tom 2. S. 147-151.

2. Semenov S.G., Davydov V.V. Matematicheskaya model' rasprostraneniya komp'yuternykh virusov v geterogennykh komp'yuternykh setyakh avtomatizirovannykh sistem upravleniya tekhnologicheskim protsessom / S.G. Semenov, V.V. Davydov // Vestnik NTU «KhPI». Sbornik nauchnykh trudov. Seriya: Informatika i podelirovanie. Khar'kov: NTU «KhPI», 2012. №38. S. 163-171.

3. Semenov S.G., Davydov V.V. Matematicheskaya model' tekhnologii rasprostraneniya zloumyshlennogo programmnogo obespecheniya v komp'yuternykh setyakh / S.G. Semenov, V.V. Davydov // Vostochno-evropeiskii zhurnal peredovykh tekhnologii. Khar'kov, 2013. Vyp. 1/4 (61). S. 11-14.

4. M.M. Williamson, J. Leveille Epidemiological model of virus spread and cleanup. HPL-2003-39 [Elektronnyi resurs. – Rezhim dostupa: http://www.hpl.hp.com/techreports /2003/HPL-2003-39.pdf (data obrashcheniya: 08.01.14)

5. Babanin, D.V. Modeli rasprostraneniya komp'yuternykh virusov na osnove tsepei Markova / D.V. Babanin // Matematicheskoe i programmnoe obespechenie vychislitel'nykh sistem: mezhvuz. sb. nauch. tr. / pod red. A.N. Pyl'kina. M.: Goryachaya liniya - Telekom, 2009. 156 s. S. 89-93.

6. Babanin D.V. Otsenka strukturnoi zashchishchennosti komp'yuternoi seti ot virusnykh atak / D.V. Babanin // Matematicheskoe i programmnoe obespechenie vychislitel'nykh sistem: mezhvuz. sb. nauch. tr. / Pod red. A.N. Pyl'kina — Ryazan': RGRTU, 2011. 224 s. S. 133-138.

7. Kemeni Dzh. Dzh. Konechnye tsepi Markova / Dzh. Dzh. Kemeni, Dzh. L. Snell. M.: Nauka. 1970. 272 s.

8. Malinetskii G.G. Nelineinaya dinamika: podkhody, rezul'taty, nadezhdy / G.G. Malinetskii, A.B. Potapov, A.V. Podlazov. M.: URSS, 2006.

УДК 004.49.5

Математическая модель технологии распространения злоумышленного программного обеспечения в гетерогенных компьютерных сетях на основе цепей Маркова

[1] Сергей Геннадьевич Семенов
[2] Вячеслав Вадимович Давыдов

[1] Национальный технический университет «Харьковский Политехнический Институт», Украина
61002, г. Харьков, ул. Фрунзе, 21
Кандидат технических наук, доцент
E-mail: s_semenov@ukr.net
[2] Национальный технический университет «Харьковский Политехнический Институт», Украина
61002, г. Харьков, ул. Фрунзе, 21
Преподаватель
E-mail: davs87@inbox.ru

Аннотация. Проведен анализ существующих подходов математического моделирования технологий рапространения злоумышленного программного обепечения в гетерогенных компьютерных сетях. Сделан вывод о целесообразности использования технологий PSIDR и PSIDDR для новых разработок. В качестве основного подхода математического моделирования было выбрано направление, связанное с графовым подходом (цепи Маркова). На основе цепей Маркова были разработаны математические модели распространения компьютерных вирусов в гетерогенной компьютерной сети, учитывающие ее топологические, архитектурные и функциональные особенности. Проведены сравнительные исследования разработанных математических моделей и построены сравнительные графики зависимости количества зараженных узлов от времени функционирования компьютерной системы при распространении эпидемии. Сделан вывод о целесообразности использования разработанных моделей при проектировании гетерогенных компьютерных сетей. Библиогр.: 8 назв., Ил.: 4.

Ключевые слова: математическая модель; злоумышленное программное обеспечение; гетерогенная компьютерная сеть; цепи Маркова.