На основі біологічного підходу математичної формалізації технічних систем розроблена математична модель технології розповсюдження зловмисного програмного забезпечення в інформаційно-телекомунікаційних та комп'ютерних мережах (модель PSIDDR). Проведено аналіз та порівняльні дослідження розробленої моделі та доведена доцільність її застосування при проектуванні комп'ютерних мереж

Ключові слова: зловмисне програмне забезпечення, інформаційно-телекомунікаційні і комп'ютерні мережі, математична модель

На основе биологического подхода математической формализации технических систем разработана математическая модель технологии распространения злоумышленного программного обеспечения в информационно-телекоммуникационных и компьютерных сетях (модель PSIDDR). Проведены анализ и сравнительные исследования разработанной модели и доказана целесообразность ее применения при проектировании компьютерных сетей

Ключевые слова: злоумышленное программное обеспечение, информационно-телекоммуникационные и компьютерные сети, математическая модель

УДК 004.49.5

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ТЕХНОЛОГИИ РАСПРОСТРАНЕНИЯ ЗЛОУМЫШЛЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ

С.Г. Семенов
Кандидат технических наук, доцент*
Контактный тел.: 050-300-76-47
E-mail: s_semenov@ukr.net
В.В. Давыдов
Аспирант*
Контактный тел.: 063-475-10-41
E-mail: davs87@inbox.ru
*Кафедра вычислительной техники и программирования
Национальный технический университет
«Харьковский политехнический институт»
ул. Фрунзе, 21, г. Харьков, Украина, 61002

1. Введение

Глобализация и интенсификация международных информационных отношений, широкое использование информационных инфраструктур практически во всех сферах жизнедеятельности современного общества приводит к существенному усложнению существующего парка информационно-телекоммуникационных и вычислительных средств, несогласованности их структурного и функционального построения, и как следствие возможному дисбалансу системы оператор-машина.

Все это расширяет возможности злоумышленников в использовании методов и средств деструктивного воздействия на информационно-телекоммуникационные и компьютерные системы (ИТКС).

В настоящее время ИТКС все чаще подвергаются серьезным угрозам в связи с постоянными атаками злоумышленного программного обеспечения (ЗПО) (например Stuxnet [1, 2], Flamer [2]). Атаки приводят к различным деструктивным воздействиям (уменьшение скорости работы вычислительной системы (сети); частичное или полное блокирование работы системы (сети); имитация физических (аппаратурных) сбоев работы вычислительных средств и периферийных устройств; переадресация сообщений; и др.).

Анализ существующих систем защиты ИТКС [3, 4] от злоумышленного программного обеспечения показал, что большинство из них связано со специализированным программным обеспечением – антивирусом. Однако, как показали исследования, данное средство борьбы с ЗПО неэффективно в условиях лавинообразного заражения ИТКС. Возникает необходимость в разработке новых методов, алгоритмов, и средств, позволяющих эффективно бороться с ЗПО в данных условиях. Решение данной проблемы невозможно без предварительного математического моделирования технологии распространения ЗПО в ИТКС [5-8].

2. Анализ литературы и постановка проблемы

Анализ литературы показал [5, 7, 8], что в настоящее время существует множество подходов математического моделирования технологий распространения ЗПО. В последнее время авторы все больше внимания обращают на биологический подход моделирования [7]. Это позволяет при необходимом уровне точности существенно снизить вычислительные затраты математического моделирования. В данном подходе следует выделить наиболее известные модели: SI (Suspected-Infected), SIR (Suspected-Infected-Recovered), SEIQR (Suspected-Exposed- Infected-Quarantined-Recovered) и PSIDR (Progressive Suspected-Infected-Detected-Recovered).

Сравнительный анализ показал, что их характерным недостатком является пренебрежение факта возможного полного уничтожения компьютерной системы

в результате атаки ЗПО (анализ примеров вирусных атак, проведенных за последние 5 лет, показал, что за последнее время участились случаи заражения и распространения ЗПО, полностью уничтожающего компьютерные системы). Подобные программные угрозы получили распространение сравнительно недавно, но ущерб, причиняемый ними, в десятки раз превышает ущерб, нанесенный компьютерными вирусами, изменяющими (уничтожающими) данные.

Пренебрежение особенностями поведения подобного ЗПО при моделировании ИТКС в значительной степени снижает общий уровень адекватности математической модели.

Поэтому актуальной научной задачей является разработка математической модели распространения злоумышленных программных угроз с учетом возможного полного уничтожения компьютерных систем.

3. Разработка PSIDDR-модели

Сравнительный анализ известных математических моделей [9,10] показал, что современные технологии распространения ЗПО наиболее адекватно описываются с помощью модели PSIDR (Progressive Suspected-Infected-Detected-Recovered). Математическая модель PSIDR [5] характеризуется наличием четырех типов объектов управления: зараженные (I), не зараженные (S), вылеченные объекты, обладающие иммунитетом (R) и найденные зараженные объекты (D).

В статье предлагается использование дополнительного состояния системы – выведение из строя объекта. Тогда с учетом данного фактора математическую модель распространения злоумышленных программных угроз можно представить в виде модели PSIDDR (Progressive Suspected Infected Detected Destructed Recovered). Данная модель характеризуется наличием четырех типов объектов управления: зараженные (I), не зараженные (S), вылеченные объекты, обладающие иммунитетом (R) и найденные зараженные объекты (D), выведенные из строя объекты (X).

Процесс воздействия злоумышленного программного обеспечения на компьютерные системы АСУ ТП и ответные реакции систем защиты на указанную угрозу в исследуемом подходе математического моделирования в общем можно разделить на два этапа:

1. Только заражение объектов (модель идентична модели SI);

2. Лечение объектов (при этом вылеченные узлы не заражаются повторно).

Исходя из указанных условий, обобщенная структура компьютерной системы на основе модели PSIDDR может быть представлена с помощью выражения:

$$N = S(t) + I(t) + D(t) + R(t) + X(t), \quad (1)$$

где: S(t) – количество уязвимых объектов;

I(t) – количество зараженных объектов;

R(t) – количество вылеченных объектов, обладающих иммунитетом;

D(t) – количество объектов, в которых обнаружен вирус;

X(t) – количество выведенных из строя узлов;

N – общее количество объектов в системе.

Схематически переходные процессы, происходящие в системе, можно представить в виде диаграммы рис. 1.

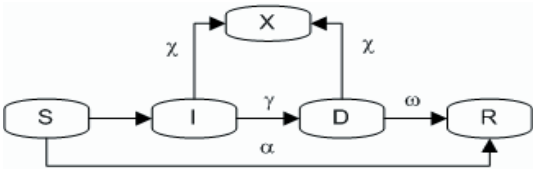

Рис. 1. Схематическая диаграмма переходов объектов системы PSIDDR

С учетом указанных особенностей функционирования компьютерной сети модель PSIDDR математически можно представить в виде системы:

$$\begin{cases} \frac{dS(t)}{dt} = -\beta S(t)I(t) - \alpha S(t) \\ \frac{dI(t)}{dt} = \beta S(t)I(t) - (\gamma + \chi)I(t) \\ \frac{dR(t)}{dt} = \omega D(t) + \alpha S(t) \\ \frac{dD(t)}{dt} = \gamma I(t) - (\omega + \chi)D(t) \\ \frac{dX(t)}{dt} = \chi I(t) + \chi D(t) \\ \frac{dS(t)}{dt} + \frac{dI(t)}{dt} + \frac{dR(t)}{dt} + \frac{dD(t)}{dt} + \frac{dX(t)}{dt} = 0, \end{cases} \quad (2)$$

где β – вероятность заражения объекта, α – вероятность иммунизации до момента заражения объекта, χ – вероятность атаки узла ЗПО с фатальными последствиями, γ – вероятность того, что ЗПО на данном узле будет выявлено, ω – вероятность лечения, S(t) – количество уязвимых объектов, I(t) – количество зараженных объектов, R(t) – количество вылеченных (с иммунитетом) объектов, X(t) – количество выведенных из строя объектов, D(t) – количество обнаруженных зараженных объектов (на первой стадии равно 0).

4. Анализ и сравнительные исследования модели PSIDDR

Используя разработанную модель PSIDDR, исследуем вероятностно-временные характеристики поведения злоумышленного программного обеспечения в компьютерной сети, состоящей из 20 узлов (объектов).

В качестве исходных параметров моделирования были выбраны числовые значения характеристик процесса распространения программных угроз, характерные реальному функционированию компьютерных сетей: α = 0,08; γ = 0,3; ω = 0,3, β = 0,2.

На рис. 2 представлены графики зависимости количества зараженных (I), выведенных из строя (X), и вылеченных (R) объектов от времени функционирования компьютерной системы, в различных начальных условиях зараженности сети.

Так, на рис. 2а приводится семейство кривых, характеризующее перечисленные процессы в условиях, когда вероятность χ = 0,01, а уровень зараже-

ния компьютерной сети на момент начала второй стадии $U=\frac{I}{N}=0{,}9$. Аналогично на рис. 2,б определены следующие начальные условия (χ = 0,1, $U=0{,}9$), на рис. 2,в – (χ = 0,1, $U=1$), на рис. 2,д – (χ = 0,01, $U=1$).

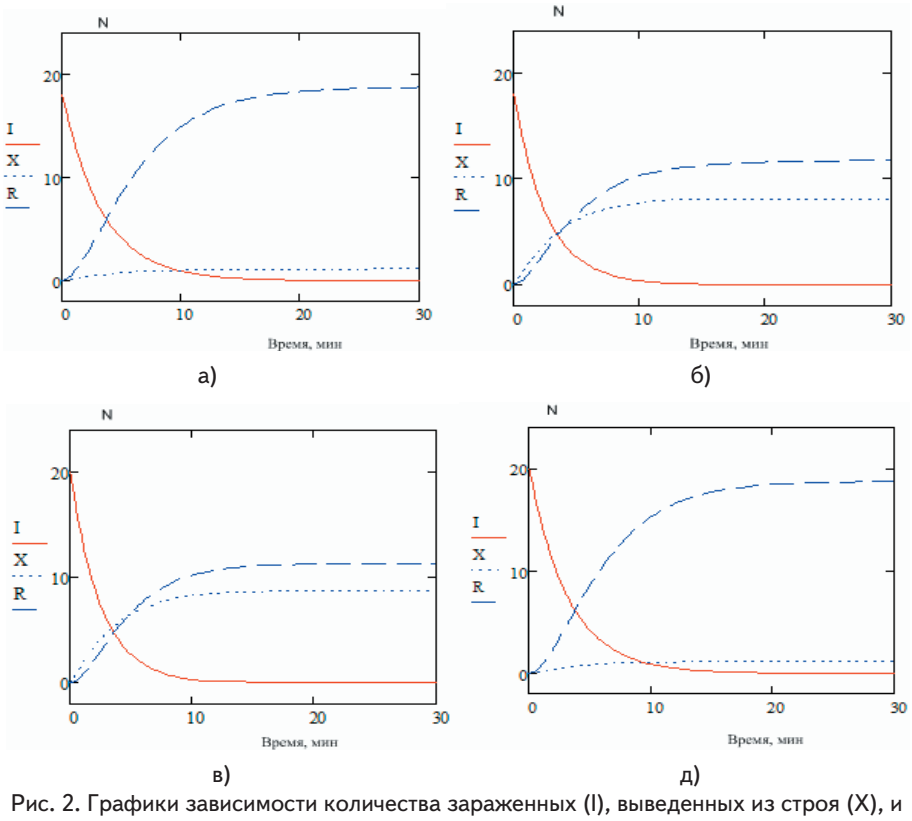

Рис. 2. Графики зависимости количества зараженных (I), выведенных из строя (X), и вылеченных (обладающих иммунитетом (R)) объектов от времени функционирования компьютерной системы

Как видно из рисунка, в первом исследуемом случае (рис. 2,а), конечное количество выведенных из строя объектов $X\approx 1$, во втором случае (рис. 2,б) это количество $X\approx 8$, в третьем (рис. 2,в) – $X\approx 9$, в четвертом (рис. 2,д) – $X\approx 1$.

Следует отметить, что представленные на рис. 2 результаты наглядно иллюстрирует общую тенденцию возрастания количества вышедших из строя объектов при увеличении уровня зараженности U, вероятности χ того, что вирус атакует узел с фатальными последствиями, и уменьшении количества R вылеченных объектов, обладающих иммунитетом.

Так, увеличение уровня зараженности U в 1,1 раза приводит к росту количества в конечном итоге вышедших из строя объектов до 1,067 раза. Уменьшение количества вылеченных объектов, обладающих иммунитетом до 1,58 раз, и увеличение вероятности χ до 10 раз, приводит к росту количества вышедших из строя объектов до 4,5 раза. С увеличением вероятности χ в 5 раз конечное количество уничтоженных узлов выросло в 4 раза.

С уменьшением количества зараженных узлов в начале второго этапа на 10% количество уничтоженных в конечном итоге узлов уменьшается так же на 10%.

Кроме того, графики рис. 2 иллюстрируют факт того, что если атака ЗПО на компьютерную сеть достигла своего результата (привела к уничтожению конкретного узла) то восстановлению данные узлы уже не подлежат.

На рис. 3 представлены кривые графиков зависимости отношения количества зараженных объектов в соответствии с моделью PSIDR к количеству зараженных объектов по модели PSIDDR ($I_{отн}=\frac{I_{PSIDR}}{I_{PSIDDR}}$), а также отношения количества вылеченных объектов, обладающих иммунитетом по модели PSIDR к количеству вылеченных объектов, обладающих иммунитетом, рассчитанных в соответствии с моделью PSIDDR ($R_{отн}=\frac{R_{PSIDR}}{R_{PSIDDR}}$) от времени распространения ЗПО в сети.

Моделирование проводилось при следующих начальных условиях, характерных условиям функционирования реальных компьютерных сетей: β=0,2, α=0,08, χ_1=0,01, χ_2=0,05 γ=0,3, ω=0,3. Как видно из графика, использование модели PSIDDR при проектировании ИТКС позволит более чем в 2 раза повысить точность оценки количества зараженных объектов и до 1,5 раз точность оценки количества вылеченных объектов, обладающих иммунитетом, по сравнению с моделью PSIDR (в установленных для моделирования начальных условиях).

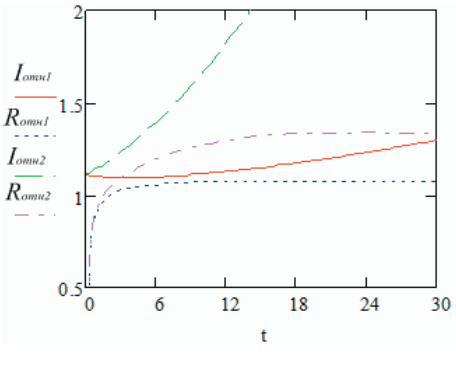

Рис. 3. Графики зависимости $I_{отн}$ и $R_{отн}$ от времени распространения ЗПО в сети

5. Выводы

Таким образом, в результате исследования разработана математическая модель технологии распро-

странения злоумышленного программного обеспечения в информационно-телекоммуникационных и компьютерных сетях (модель PSIDDR).

Анализ и сравнительные исследования модели PSIDDR показали соизмеримость результатов моделирования с известной моделью PSIDR в условиях низкой вероятности атаки узла ЗПО с фатальными последствиями, и существенное (более чем в 2 раза) повышение точности результатов моделирования в условиях воздействия ЗПО, уничтожающего аппаратную составляющую ИТКС.

Приведенные факты подтверждают целесообразность использования разработанной модели PSIDDR при проектировании ИТКС.

Литература

1. A. Matrosov, E. Rodionov, D. Harley “Stuxnet under microscope”. Доступен на http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf (Последний доступ 16 декабря 2012).
2. S. Cobb «Stuxnet, Flamer, Flame, Whatever Name: There’s just no good malware». Доступен на http://blog.eset.com/2012/06/03/stuxnet-flamer-flame-whatever-name-there-is-no-good-malware (Последний доступ 16 декабря 2012).
3. Zesheng Chen, Lixin Gao, Kevin Kwait. Modeling the spread of active worms. INFOCOM 2003. Доступен на http://www.ieee-infocom.org/2003/papers/46_03.PDF (Последний доступ 16 декабря 2012).
4. K. Rohloff , T. Basar, Stochastic Behavior of Random Constant Scanning Worms [Text] / K. Rohloff, T. Basar // Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on 17-19 Oct. 2005, pp. 339 – 344.
5. Котенко, И.В. Аналитические модели распространения сетевых червей [Текст] / И.В. Котенко, В.В. Воронцов // Труды СПИИРАН. – СПб: Наука, 2007. - Вып. 4. – С. 208-224.
6. F. Cohen, “Computer viruses, theory and experiments,” Computers & Security, vol. 6, 1987, pp. 22-35.
7. Jeffrey O. Kephart, Steve R. White, Directed-Graph Epidemiological Model of Computer Viruses // IEEE Symposium on Security and Privacy, 1991. –P.343. Доступен на http://www.research.ibm.com/antivirus/SciPapers/Kephart/VIRIEEE/virieee.gopher.html (последний доступ 16 декабря 2012).
8. M.M. Williamson, J. Leveille Epidemiological model of virus spread and cleanup. HPL-2003-39. Доступен на http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf (последний доступ 16 декабря 2012).
9. Давыдов, В.В. Сравнительный анализ моделей распространения компьютерных вирусов в автоматизированных системах управления технологическим процессом [Текст] / В.В. Давыдов // Системи обробки інформації. - Харків: ХУПС, 2012. - Вип. 3(101), Том 2. - С. 147-151.
10. Семенов, С.Г. Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом [Текст] / С.Г. Семенов, В.В. Давыдов // Вісник Національного технічного університету «ХПІ». Збірник наукових праць. Серія: Інформатика та моделювання. – Харків: НТУ «ХПІ», 2012. - Вип. 38. - С. 163-171.

Abstract

Previous researches indicate that the cases of malicious software infection and spread, which completely destroy computer systems, have become more frequent. Such software threats have proliferated recently but their damage ten times exceeds the damage caused by computer viruses which destroy data.

Therefore, the development of mathematical model of the malicious software threats spreading with the possibility of complete computer systems destruction in order to localize them is a topical scientific task.

In this article we propose a new mathematical model of malicious software spreading technology based on biological approach. It is based on PSIDR (Progressive Suspected-Infected-Detected-Recovered) model and named PSIDDR (Progressive Suspected-Infected-Detected-Destructed-Recovered).

The analysis and comparative investigation of the developed model were processed and proved the expediency of its installation in stage of computer networks designing. Also the analysis and comparative investigation showed commensurability results of modeling with the known PSIDR model in low probability of malicious software attack with fatal consequences. Also the results showed a significant (more than 2 times) increase in accuracy of the simulation results in conditions of malicious software destructing ITCS (Informational Tele-Communication System) hardware components

Keywords*: malicious software, information and telecommunication and computer networks, the mathematical model*