УДК 004.056.57

МОДЕЛИРОВАНИЕ КОМПЬЮТЕРНЫХ ВИРУСНЫХ ЭПИДЕМИЙ

В. А. Минаев, М. П. Сычев, Е. В. Вайц, А. Э. Киракосян

В статье описана системно-динамическая модель распространения компьютерных вирусов на примере Wanna Cry и других современных вирусных программ. Модель реализована в имитационной среде Anylogic. Показана её высокая согласованность с эмпирическими данными (коэффициенты детерминации не менее 86%). Модель позволяет осуществлять прогноз вирусных эпидемий, проигрывать различные сценарии их развития, дает возможность подготовки управленческих решений для оптимального использования ресурсов при обеспечении информационной безопасности

Ключевые слова: компьютерный вирус, системно-динамическая модель, имитационное моделирование, управление, информационная безопасность

Введение

Многообразие вирусных атак, способных нанести значительный ущерб организациям и конкретным пользователям, определяет актуальность проблемы исследования вирусных эпидемий в компьютерных сетях. Для решения задач прогнозирования указанных эпидемий и выработки управленческих решений по противодействию им необходимо совершенствование математического аппарата, позволяющего адекватно моделировать процессы распространения вирусов в компьютерных сетях.

На сегодняшний день накоплен значительный опыт в указанном направлении, отражающий самые различные сферы исследований [1-9]. В качестве базового математического аппарата в них выбраны модели распространения обычных эпидемий.

Однако до сих пор недостаточно раскрыта возможность применения имитационного моделирования, которое предоставляет широкий спектр возможностей по анализу эпидемий в компьютерных сетях, их прогнозированию и управлению ими. Имитационные модели позволяют достаточно эффективно учитывать большое количество причинно-следственных связей между объектами.В качестве метода имитационного моделирования перспективным выступает метод системной динамики, предложенный и обоснованный Дж. Форрестером в 1950-х годах [6]. Основными элементами системно-динамических моделей являются уровни, отражающие различного рода накопления, происходящие в модели, и темпы, определяющие динамику моделируемых процессов.

В настоящей статье для обоснования, построения и реализации модели распространения компьютерных вирусов в теоретическом плане использовались принципы системной динамики [10], в программно-методическом – возможности имитационной платформы Anylogic [11], в прикладном – статистические данные о динамике прибыли злоумышленников в результате заражения компьютеров вирусом WannaCry, представленные компанией Elliptic на сайте https://www.elliptic.co/, а также статистические данные о распространении вирусов Android.Oldboot и BackDoor.Finder, представленные на портале компании Dr.Web.

Компания Elliptic занимается идентификацией незаконной деятельности, использующей технологию «блокчейн биткоин». Напомним, что компьютерный вирус Wanna Cry требовал от пользователей заплатить за расшифровку их файлов именно в биткоинах.

Системно-динамическое моделирование вирусных эпидемий

Динамика прибыли злоумышленников в результате распространения компьютерного

Минаев Владимир Александрович - МГТУ им. Н.Э. Баумана, д. т. н., профессор, e-mail: m1va@yandex.ru
Сычев Михаил Павлович - МГТУ им. Н.Э. Баумана, д. т. н., профессор, e-mail: mpsichov@sm.bmstu.ru
Вайц Екатерина Викторовна - МГТУ им. Н.Э. Баумана, ст. преподаватель, e-mail: vaitcev@yandex.ru
Киракосян Артур Эрнестович - МГТУ им. Н.Э. Баумана, аспирант, e-mail: kirakosyan@i-teco.ru

вируса Wanna Cry описана с помощью системно-динамической модели (рис. 1), которая представлена в обозначениях, предложенных Дж. Форрестером [7].

Расшифровка условных обозначений, используемых в модели, представлена в табл. 1.

Табл. 1

Условные обозначения, используемые в модели

Условные обозначения	**Название (единицы измерения)**
D	Итоговая прибыль злоумышленников ($ *тыс.*)
S	Количество компьютеров, подверженных заражению (*шт.*)
IU	Темп устранения уязвимости на зараженных компьютерах (*шт./час*)
SU	Темп устранения уязвимости на незараженных компьютерах (*шт./час*)
D_1	Потенциальная прибыль злоумышленников с одного компьютера ($ *тыс.*)
p	Вероятность перечисления денежных средств в случае заражения компьютера
b	Частота заражения (*шт./час*)
n	Общее количество компьютеров в сети (*шт.*)
u	"Нормальная" скорость устранения уязвимости *(доля/час)*
I	Количество зараженных компьютеров (*шт.*)
U	Количество компьютеров, на которых устранена уязвимость *(шт.)*
OD	Темп увеличения прибыли злоумышленников ($ *тыс./час*)
SI	Темп заражения компьютеров (*шт./час*)

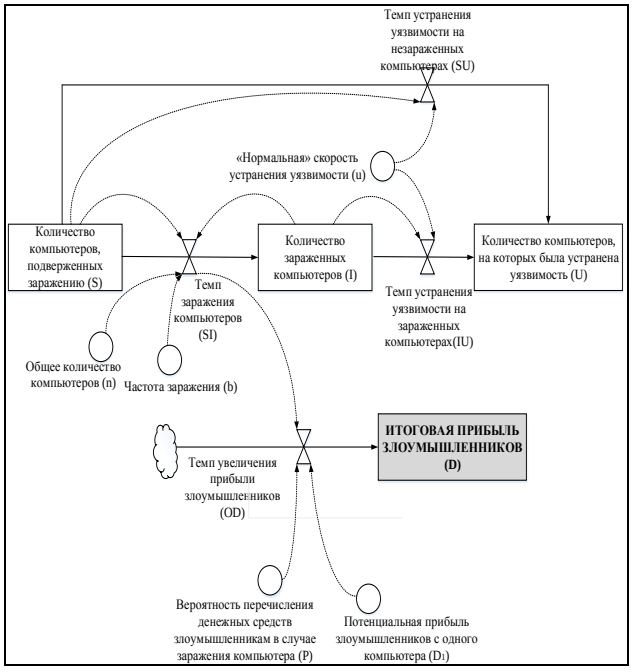

Рис. 1. Потоковая диаграмма системно-динамической модели прибыли злоумышленников в результате распространения компьютерного вируса Wanna Cry

Модель описывается с помощью следующей системой уравнений:

$$\begin{cases} \dfrac{dD}{dt} = OD(t) \\ OD(t) = D_1 \cdot p \cdot SI(t) \\ SI(t) = \dfrac{dI}{dt} = \dfrac{b \cdot I(t) \cdot S(t)}{n} \\ \dfrac{dS}{dt} = -SI(t) - SU(t) \\ \dfrac{dU}{dt} = IU(t) + SU(t) \\ IU(t) = u \cdot I(t) \\ SU(t) = u \cdot S(t) \end{cases} \quad (1)$$

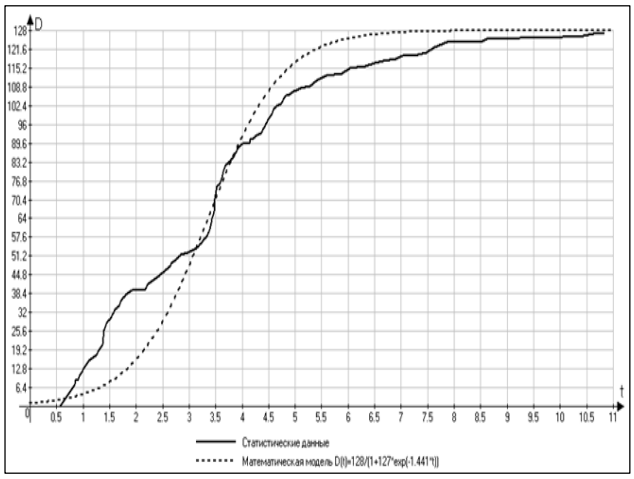

Рис. 2. Динамика прибыли злоумышленников, распространявших вирус Wanna Cry

Приведем зависимость *D(t)*, полученную на основе математической модели (рис. 2. – пунктирная линия). Статистические данные о динамике прибыли злоумышленников отображены сплошной линией. Коэффициент детерминации R^2 равен 92%, что отражает высокую объясняемость предложенной модели.

Тем не менее, из рис. 2 видно, что в период до 3 дней модель отстает от реальной динамики прибыли злоумышленников (в этот период они требовали за «решение» проблем $300), а по прошествии 4 дней начинает опережать ее (в этот период цена «решения» возросла до $600).

Именно изменение требований злоумышленников привело к тому, что параметры модели были выбранными непостоянными во времени.

Так, параметр *p* (вероятность перечисления злоумышленникам денежных средств в случае заражения компьютера) в начале распространения вирусной эпидемии (до трех обозначенных в ультиматуме дней) принимает б*о*льшие значения ввиду неожиданности нападения, важности зашифрованной вирусом информации и неоправданных ожиданий устранения последствий вирусной атаки за меньшие деньги. Но затем у пользователей стало укрепляться понимание того, что последствия вирусной атаки вовсе не будут устранены после перечисления денежных средств (ведь у злоумышленников – другие мотивы, другая психология, другое понимание моральных и этических ценностей), и вероятность решить проблему «за деньги», “договориться” со злоумышленниками стала падать. Таким образом, эпидемический процесс в модели целесообразно разбить на два этапа, различающихся параметрами моделей (рис. 3). В этом случае коэффициент детерминации возрос в среднем до 96%, отражая повышение достоверности предложенной модели.

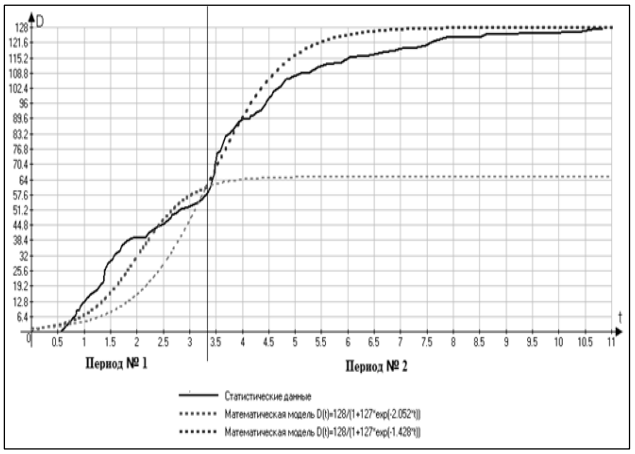

Рис.3. Динамика прибыли злоумышленников в результате заражения компьютерной сети вирусом Wanna Cry с учетом двух периодов эпидемии

В рамках предложенной системно-динамической модели (с постоянными во времени параметрами) описаны статистические данные о динамике распространения компьютерных вирусов Android.Oldboot и BackDoor.Finder, представленные на портале компании Dr.Web (рис. 4, 5).

Коэффициент детерминации составил соответственно 86% и 93%, отражая весьма высокую объясняемость модели.

Выводы

1. Системно-динамический подход к моделированию вирусных эпидемий с использованием возможностей имитационной платформы Anylogic позволяет с достаточными высокой точностью и содержательным смыслом описать динамику распространения компьютерных вирусов.

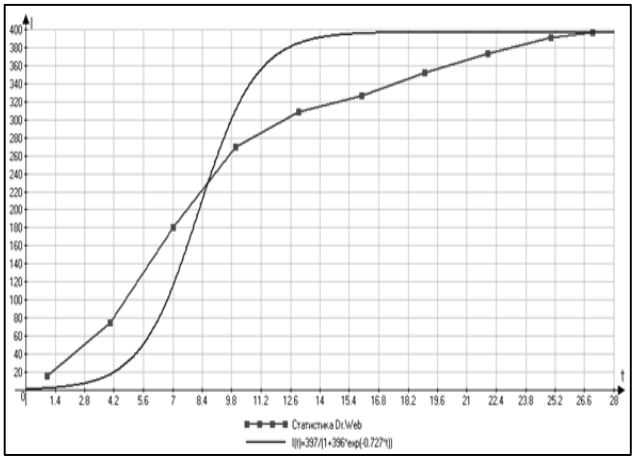

Рис. 4. Результаты моделирования динамики роста бот-сети Android.Oldboot

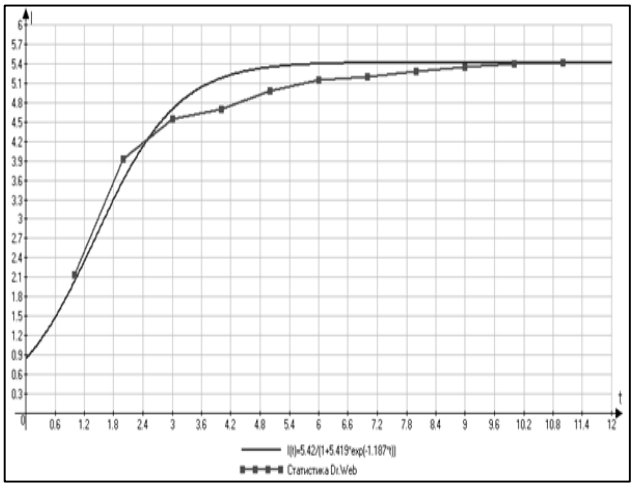

Рис. 5. Результаты моделирования динамики роста бот-сети BackDoor.Finder

2. Разработанные системно-динамические модели позволяют осуществлять прогнозирование и оценку характеристик вирусных эпидемий, рассматривать различные гипотезы относительно их причин и факторов.

3. Инструментарий имитационной системы Anylogic позволяет более детально

рассмотреть процессы вирусных эпидемий, включая особенности управления антивирусными ресурсами служб, обеспечивающих безопасность компьютерных систем.

Литература

1. Котенко, И. В., Воронцов В. В. Аналитические модели распространения сетевых червей // Труды СПИИРАН. СПб.: Наука. 2007. – С. 208-224.

2. Гусаров, А. Н., Жуков, Д. О., Косарев, А. В. // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2010. №1. С. 112-120.

3. Тесалова, О. Т., Новикова, Н. Ф., Минаев, В. А., Кононенко, В. И. Моделирование динамики заболеваемости сифилисом // Вестник дерматологии и венерологии. 1981. № 4. – С. 21-24.

4. Тесалова, О. Т., Минаев, В. А., Лещенко, Б. М., Новикова, Н. Ф. Моделирование заболеваемости трихофитией // Вестник дерматологии и венерологии. 1989. № 9. – С. 32-38.

5. Минаев, В. А. Кадровые ресурсы органов внутренних дел: современные подходы к управлению. М.: Академия МВД СССР, 1991. – 163 с.

6. Минаев, В. А., Вайц, Е. В., Грачева, Ю. В., Власенко, О. А., Мареев, К. И., Киракосян, А. Э. Моделирование вирусных атак в компьютерных сетях с различной топологией / Сборник трудов XXVI Всероссийской научной конференции «Информатизация и информационная безопасность правоохранительных органов». М.: Академия управления МВД России. 7 июня 2017. – С. 293-296.

7. Минаев, В.А., Сычёв, М.П., Вайц, Е.В., Грачёва, Ю.В. Моделирование вирусных эпидемий в компьютерной сети с использованием принципов системной динамики / Материалы Всероссийской научно-технической конференции “Математические методы и информационные технологии управления в науке, образовании и правоохранительной сфере”, 27–28 апреля 2017 г. Под общ. ред. В. А. Минаева. Рязань: Академия ФСИН России, 2017. – С. 89-93.

8. Минаев, В.А., Сычёв, М.П., Вайц, Е.В., Грачёва, Ю.В. Моделирование угроз информационной безопасности с использованием принципов системной динамики // Вопросы радиоэлектроники. 2017. №6. – С. 75-82.

9. Минаев В.А., Вайц Е.В., Корячко А.В., Киракосян А.Е. Системно-динамическое моделирование распространения компьютерных вирусов // Технологии техносферной безопасности: Интернет-журнал. Вып. 3 (73). 2017. URL: http://academygps.ucoz.ru/ttb/ 2017-3/2017-3.html.

10. Форрестер, Д. Основы кибернетики предприятия (индустриальная динамика). Москва: Прогресс, 1971. – 340с.

11. Маликов, Р. Ф. Практикум по имитационному моделированию сложных систем в среде AnyLogic 6: учебное пособие. Уфа: Изд-во БГПУ, 2013. – 296 с.

ФГБОУ ВПО “Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)”
Bauman Moscow State Technical University

SIMULATION COMPUTER VIRUS EPIDEMICS

V. A. Minaev, M. P. Sychev, E. V. Vaitc, A. E. Kirakosyan

The article deals with the process of system dynamics modeling of computer viruses spreading as Wanna Cry and other modern viral programs. The model is implemented in the Anylogic simulation platform. It shows high consistency with empirical data (the coefficients of determination no less than 86 %). Models allow the prediction of viral epidemics, to simulate different scenarios of their development, to prepare of management decisions for optimum use of resources while ensuring information security

Key words: computer virus, system-dynamic model, simulation, management, information security