УДК 004.49.5

Мохамад Абу Таам Гани, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов

Кировоградский национальный технический университет, Кировоград

СРАВНИТЕЛЬНЫЕ ИССЛЕДОВАНИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ТЕХНОЛОГИИ РАСПРОСТРАНЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Проведены сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях. Описанная модель, в отличие от известных, учитывает ключевую информацию о состояниях телекоммуникационных узлов в процессе деструктивных воздействий компьютерных вирусов, а также фактор использования «облачного» антивирусного обеспечения в процессе лечения, что позволило повысить точность полученных результатов по сравнению с известными до 1,4 раза.

Ключевые слова: *информационно-телекоммуникационные сети, компьютерные вирусы, облачные антивирусы, GERT-модель, математическая модель PSIDDR.*

Введение

Постановка проблемы исследования. Современное развитие информационно-телекоммуникационных сетей (ИТС) и применяемых компьютерных технологий привело к появлению качественно новых услуг и сервисов в информационной сфере, внедрению передовых технологий обработки и передачи данных и их доступности широкой пользовательской аудитории [1 – 10]. В то же время интенсивное развитие современных компьютерных технологий привело к появлению новых угроз безопасности информации, возникновению новых форм и способов несанкционированного доступа к вычислительным ресурсам информационно-телекоммуникационных сетей [1 – 10].

Одной из актуальных угроз в информационно-телекоммуникационных сетях является распространение компьютерных вирусов. Компьютерный вирус – это специально написанная, небольшая по размерам программа (т.е. некоторая совокупность выполняемого кода), которая может "приписывать" себя к другим программам ("заражать" их), создавать свои копии и внедрять их в файлы, системные области компьютера и т.д., а также выполнять различные нежелательные действия на компьютере. На данный момент существуют следующие классические виды вирусов:

– Черви – зловредные программы обычно пролазят на компьютер пользователя через дыру в Интернет броузере или операционной системе. Запускаются, как правило, автоматически или при наведении мышки на него. Часто распространяются через видеосервисы, например, YouTube. Удалить антивирусом получается не всегда, приходится удалять вручную. Microsoft постоянно выпускает заплатки к обнаруженным дырам в операционной системе Windows и своем любимом броузере Internet Explorer. Поэтому нужно постоянно скачивать обновления с сайта компании Microsoft, тем самым закрывая дыры, через которые распространяются черви.

– Трояны – программный код весом в несколько десятков килобайт, а то и байт, который запускается при запуске софта, скаченного с неблагонадежного сайта или при генерировании пиратского серийника для какой-нибудь программы. Задача трояна – украсть всевозможные пароли, личные данные пользователя, отчет о всех нажатых клавишах и при первом же выходе в Интернет отправить украденные данные злоумышленнику.

– Бутовые вирусы – заражают загрузочную область жестких дисков, тем самым прекращая загрузку операционной системы.

– Макровирусы – были разработаны для распространения через документы Microsoft World. Например, при открытии таблицы в документе запускается вирус-макрос, написанный на языке Visual Basic.

– Spyware – программы шпионы Спайвары. Очень глубоко внедряются в вашу систему и сохраняют о вас всю информацию, которую затем отправляют по электронной почте своему хозяину. Бывают и легальные Спайвары, которые призваны следить за детьми – какие сайты они посещают.

– Adware – оригинальный тип вируса, который попадает к вам в виде конфигурационных файлов для Интернет броузера или почтовой программы и показывает вам рекламу, за которую хозяин этого вируса получает деньги от рекламодателя.

– Root-kit – это целый набор инструментов, предназначенный для взлома вашей операционной системы.

– Полиморфные вирусы – очень опасный тип вируса, который, попадая на компьютер, сразу старается изменить свой код, маскируясь под легальную программу. Данный тип вируса тяжело отследить антивирусу, так он запускается не сразу, а постепенно, внедряясь в легальную программу.

© Мохамад Абу Таам Гани, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов

– Файловый вирус – считается классическим вирусом, который добавляется сразу в несколько файлов и выполняет свою зловредную функцию, запускаясь при включении компьютера и попадая в оперативную память.

В работе предлагается использовать математический аппарат GERT-модели ИТС и математической модели PSIDDR для проведения сравнительного исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях. Полученные результаты могут быть использованы для совершенствования механизмов антивирусной защиты в информационно-телекоммуникационных сетях.

Анализ последних исследований и публикаций. Анализ литературы показал [1 – 11], что в настоящее время существует множество подходов математического моделирования технологий распространения вредоносного программного обеспечения (ВПО). В последнее время авторы все больше внимания обращают на биологический подход моделирования [1 – 2, 7 – 11]. 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 ВПО (анализ примеров вирусных атак, проведенных за последние 5 лет, показал, что за последнее время участились случаи заражения и распространения ВПО, 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 ВПО при моделировании информационно-телекоммуникационных сетей (ИТКС) в значительной степени снижает общий уровень адекватности математической модели.

Поэтому актуальной научной задачей является сравнительное исследование математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях.

Математическая GERT-модель технологии передачи метаданных в облачные антивирусные системы

Проведенные исследования основных подходов математического моделирования показали, что наиболее удобной, наглядной и многосторонней формой описания технологии передачи метаданных в облачные антивирусные системы является граф алгоритмов на основе GERT-сети.

Для рассматриваемого в статье примера под графом алгоритмов понимается орграф G = (X, U), вершины x_i которого отображают частные реализации i-х алгоритмов системы. Вершинам графа приписывается вес, соответствующий времени реализации алгоритма. (В отдельных случаях это может быть вероятность показания на тот или иной выход узлов графа, требующаяся для выполнения память, ошибки определения тех или иных величин, связанных с реализацией алгоритма и т.д.). Частные реализации алгоритмов в рассматриваемом графе GERT-сети отождествляется дугами графа с определенными условными вероятностями и производящими функциями моментов ветви.

Типовая модель алгоритмов формирования и передачи метаданных в облачные антивирусные системы представлена на рис. 1. Воспользуемся представленными на рис. 1 данными для разработки GERT-модели ИТС в процессе передачи метаданных в облачные антивирусные системы.

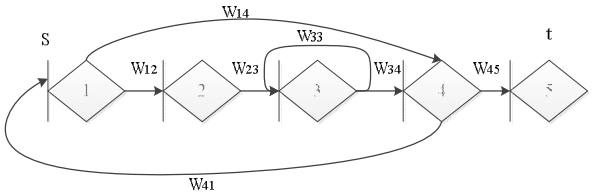


Рис. 1. Модель алгоритмов формирования и передачи метаданных в облачные антивирусные системы

Эта модель может быть описана следующим образом. Ветвь (1,2) интерпретирует время формирования метаданных (сигнатур). Ветвь (2,3) задает время передачи кадра (пакета) метаданных от передатчика к трансляторам (маршрутизаторам). Ветвь (3,3) отображает возможное неисправное состояние транслирующего коммутационного оборудования (маршрутизаторов) на выбранных маршрутах. Ветвь (3,4) описывает время коммутации кадра (пакета) в телекоммуникационном оборудовании. Ветви (4,1) и (4,5) задают случайное время передачи квитанции о правильности (ошибке) доставки кадров (пакетов) в соответствии с протоколом транспортного уровня (TCP).

Узел 5 отражает состояние системы в момент анализа метаданных на предмет наличия ВПО.

В ряде практических случаев с целью повышения вероятности выявления ВПО существует необходимость антивирусного анализа не сформированных на оконечном оборудовании сигнатур, а данных, хранимых на этом оборудовании в полном объеме. Этой ситуации соответствует ветвь (1,4).

Ветви (3,4), (4,1) и (4,5) целесообразно описывать идентичными параметрами распределения, так

как они задают схожие операции передачи данных небольшого объема.

Анализ ряда работ [1 – 6], а также проведенные исследования процесса передачи данных в мультисервисных телекоммуникационных сетях позволили сформировать характеристики ветвей и параметры распределения в виде, представленном в табл. 1.

Анализ данных, представленных в табл. 1, показал высокую структурную сложность разрабатываемой GERT-сети. Особенно остро данная проблема фиксируется на участке, сформированном из узлов 2-3-4 (ветви (2,3), (3,3)).

Таблица 1

Характеристики ветвей модели

№ п/п	Ветвь	W-функция	Вероятность	Производящая функция моментов
1	(1,2)	W_{12}	p_1	$\lambda_1/(\lambda_1-s)$
2	(1,4)	W_{14}	$1\text{-}p_1$	$\lambda_2/(\lambda_2-s)$
3	(2,3)	W_{23}	p_2	$\lambda_3/(\lambda_3-s)$
4	(3,3)	W_{33}	p_3	$\lambda_4/(\lambda_4-s)$
5	(3,4)	W_{34}	1- p3	$\lambda_5/(\lambda_5-s)$
6	(4,5)	W_{45}	p_4	$\lambda_5/(\lambda_5-s)$
7	(4,1)	W_{41}	1- p_4	$\lambda_5/(\lambda_5-s)$

С целью упрощения рассматриваемой на рис. 1 модели воспользуемся методикой эквивалентных упрощающих преобразований, описанной в работах [3, 4]. В результате упрощающих преобразований сформируем GERT-сеть, представленную на рис. 2. Как видно из этого рисунка, в результате упрощающих преобразований ветви (2,3) и (3,3) были заменены на эквивалентную ветвь. Обновленные данные характеристик ветвей сети представлены в табл. 2.

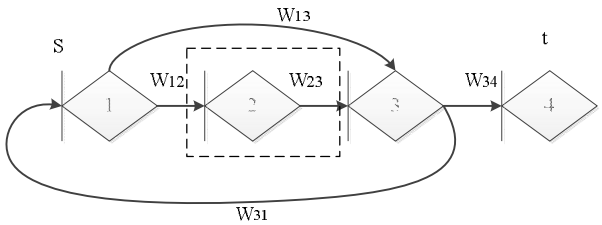


Рис. 2. Упрощенная модель алгоритмов формирования и передачи метаданных в облачные антивирусные системы

Таблица 2

Характеристики ветвей модели

№ п/п	Ветвь	W-функция	Параметр распределения
1	(1,2)	W_{12}	$p_1\lambda_1/(\lambda_1-s)$
2	(1,3)	W_{13}	$(1\text{-}p_1)\,\lambda_2/(\lambda_2-s)$
3	(2,3)	W_{23}	$\dfrac{p_2\lambda_3}{(\lambda_3-s)((\lambda_4-s)-p_3\lambda_4)}$
4	(3,4)	W_{34}	$p_4\lambda_5/(\lambda_5-s)$
5	(3,1)	W_{31}	$(1-p_4)\lambda_5/(\lambda_5-s)$

В соответствии с характеристиками ветвей GERT-сети определим эквивалентную W-функцию времени передачи файла как:

$$W_E(s)=\frac{W_{13}W_{34}+W_{12}W_{23}W_{34}}{1-W_{13}W_{31}-W_{12}W_{23}W_{31}}=$$

$$=\frac{\left(\dfrac{p_4\lambda_5q_1\lambda_1(\lambda_1-s)(\lambda_3-s)((\lambda_4-s)-p_3\lambda_4)+p_1\lambda_1p_4\lambda_5p_2\lambda_3(\lambda_2-s)}{(\lambda_2-s)(\lambda_5-s)(\lambda_3-s)((\lambda_4-s)-p_3\lambda_4)}\right)}{\left(\dfrac{(\lambda_1-s)(\lambda_2-s)(\lambda_5-s)(\lambda_3-s)((\lambda_4-s)-p_3\lambda_4)-q_1\lambda_2q_4\lambda_5(\lambda_1-s)(\lambda_3-s)((\lambda_4-s)-p_3\lambda_4)-p_1\lambda_1q_4\lambda_5p_2\lambda_3(\lambda_2-s)}{(\lambda_2-s)(\lambda_1-s)(\lambda_5-s)(\lambda_3-s)((\lambda_4-s)-p_3\lambda_4)}\right)},$$

где $1-p_1=q_1$, $1-p_2=q_2$, $1-p_3=q_3$, $1-p_4=q_4$.

Проведенные исследования показали, что в сложных GERT-сетях с возможными циклами отсутствуют простые методы нахождения особых точек функции $\Phi_E(z)$ замены действительных переменных $(z=-i\varsigma)$, где ς – действительная переменная. Связано это с тем, что для нахождения особых точек необходимо решать нелинейные уравнения, и чем сложнее структура GERT-сети, тем сложнее и исходное уравнение [3, 4]. Поэтому в ходе моделирования выполняя комплексное преобразование получим:

$$\Phi(z)=\frac{uz^3-kz^2+wz+h}{\left(z^3+vz^2+rz+c\right)}, \qquad (1)$$

где

$$u=p_4\lambda_5q_1\lambda_2,$$

$$k=p_4\lambda_4q_1\lambda_2\left(p_3\lambda_4-\lambda_3-\lambda_1-\lambda_4\right),$$

$$w=p_4\lambda_5q_1\lambda_2\times$$

$$\times\left(p_3\lambda_3\lambda_4-\lambda_1\lambda_3-\lambda_3\lambda_4-\lambda_1\lambda_4+p_3\lambda_1\lambda_4\right),$$

$$h=p_4\lambda_4q_1\lambda_1\lambda_2\lambda_3\lambda_4q_3,$$

$$v=\lambda_3-\lambda_4-\lambda_2+q_1q_4\lambda_2\lambda_5+p_3\lambda_4,$$

$$r=\lambda_3\lambda_4+\lambda_3\lambda_2-q_1\lambda_2q_4\lambda_5\lambda_3-p_3\lambda_3\lambda_4+\lambda_2\lambda_4-$$

$$-q_1\lambda_2q_4\lambda_5\lambda_4-p_3\lambda_2\lambda_4+q_1\lambda_2q_4\lambda_5p_3\lambda_4,$$

$$c=\lambda_3\lambda_4\lambda_2-q_1\lambda_2q_4\lambda_3\lambda_4\lambda_5-p_3\lambda_3\lambda_4\lambda_2+$$

$$+q_1\lambda_2q_4\lambda_3\lambda_4p_3.$$

Из выражения (1) видно, что функция $\Phi(z)$ имеет только простые полюсы, определяемые корнями уравнения $z^3+vz^2+rz+c=0$. В этом случае

плотность распределения вероятностей времени передачи сообщения равна:

$$\varphi(x)=\frac{1}{2\pi i}\int_{-i\infty}^{i\infty} e^{zx}\frac{uz^3-kz^2+wz+h}{\left(z^3+vz^2+rz+c\right)}dz. \qquad (2)$$

Используя специализированный математический пакет Mathcad, определим простые полюсы z функции $\Phi(z)$ и найдем плотность распределения вероятностей $\varphi(x)$ времени передачи метаданных в «облачные» антивирусные системы. При этом в качестве начальных данных определим следующие параметры ветвей GERT-сети:

$p_1=0,9$, $p_2=0,99999$, $p_3=0,99999$, $p_4=0,99999$,

$\lambda_1=1$, $\lambda_2=0,099$, $\lambda_3=0,9$, $\lambda_4=0,5$, $\lambda_5=0,4$.

Для указанного примера функция $\Phi(z)$ имеет простые полюса:

$$z:=\begin{pmatrix}-0.67\\0\\-0.117\end{pmatrix}.$$

В соответствии с формулой (2) $\varphi(x)$ равна:

$$\frac{1}{z}\,0.159155\times 2.71828^{(-0.0835025-0.364433\,i)\,z}\left(z\,2.71828^{(0.920508+0.364433\,i)\,z}\,\mathrm{Ei}((x-0.837005)\,z)\right.$$
$$(1.02026\,h-0.714769\,k+0.85396\,v+0.598265)+$$
$$2.71828^{(0.728866\,i)\,z}\,z\,\mathrm{Ei}((x+(0.0835025-0.364433\,i))\,z)$$
$$(-(0.142616-0.131097\,i)\,k-(0.42698+0.293502\,i)\,v+$$
$$(0.0358675+0.0629208\,i)+(-0.510128+1.28851\,i)\,h)-$$
$$(0.510128+1.28851\,i)\,h\,z\,\mathrm{Ei}((x+(0.0835025+0.364433\,i))\,z)-$$
$$(0.142616+0.131097\,i)\,k\,z\,\mathrm{Ei}((x+(0.0835025+0.364433\,i))\,z)\cdot$$
$$(0.42698-0.293502\,i)\,v\,z\,\mathrm{Ei}((x+(0.0835025+0.364433\,i))\,z)+$$
$$(0.0358675-0.0629208\,i)\,z\,\mathrm{Ei}((x+(0.0835025+0.364433\,i))\,z)$$
$$\left.2.71828^{z\,(x+(0.0835025+0.364433\,i))}\right)+\mathrm{constant}$$

На рис. 3. представлен график плотности распределения времени передачи мета данных.

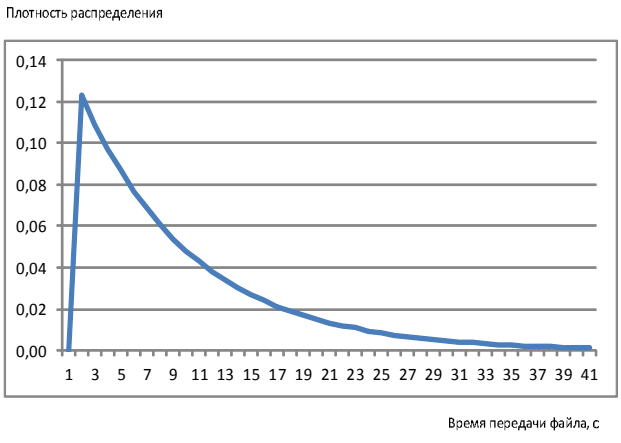


Рис. 3. Плотность распределения времени передачи метаданных в облачные антивирусные системы

Как видно из этого рисунка, максимальные значения плотности распределения времени формирования и передачи приходится на промежуток от 1 до 3 с.

Сравнительное исследование разработанной математической модели

Проведем сравнительные исследования разработанной математической модели технологии распространения компьютерных вирусов в ИТС. Для такого исследования и соответственно оценки в качестве эталонной выберем математическую модель PSIDDR, представленную в работах [1, 2] на основе биологического подхода моделирования. По данным источников [1, 2] указанная математическая модель наиболее адекватно описывает процесс распространения компьютерных вирусов и учитывает пять возможных состояний узлов ИТС в процессе их функционирования в условиях внешних деструктивных воздействий.

Приведем описание математической модели PSIDDR.

Проведенные исследования показали, что в последнее время участились случаи заражения и распространения злоумышленного программного обеспечения, полностью уничтожающего компьютерные системы. Подобное злоумышленное ПО получили распространение сравнительно недавно, но ущерб, причиняемый ними, в десятки раз превышает ущерб, нанесенный компьютерными вирусами изменяющими (уничтожающими) данные. Поэтому пренебрежение особенностями поведения злоумышленного программного обеспечения, уничтожающего компьютерную систему, при моделировании ИТС в значительно степени снижает общий уровень адекватности математической модели. В то же время, отсутствие учета возможных последствий заражения подобного рода злоумышленным программным обеспечением при проектировании, может привести к уничтожению как отдельных сегментов ИТС, так и ИТС в целом. Поэтому актуальной задачей является разработка математической модели распространения злоумышленного программного обеспечения с учетом возможного полного уничтожения компьютерных систем.

Для решения указанной проблемы предлагается использование дополнительного состояния системы – выведение из строя объекта. Тогда с учетом данного фактора математическую модель распространения злоумышленного программного обеспечения можно представить в виде модели PSIDDR (Progressive Suspected Infected Detected Death Recovered). Исходя из выделенных в [1, 2] данных, в математической модели PSIDDR обобщенная структура ИТС может быть представлена с помощью выражения [1, 2]:

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

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.

С учетом указанных особенностей функционирования ИТС модель PSIDDR математически можно представить в виде системы (1), где:

β – частота заражения,

α – вероятность иммунизации до стадии заражения,

χ – вероятность того, что вирус атакует узел с фатальными последствиями,

γ – вероятность того, что вирус на данном узле будет выявлен,

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),

N – общее количество объектов в системе.

$$\begin{cases} \frac{dS(t)}{dt} = -\beta\frac{S(t)I(t)}{N} - \alpha S(t); \\ \frac{dI(t)}{dt} = \beta\frac{S(t)I(t)}{N} - (\gamma+\chi)I(t); \\ \frac{dR(t)}{dt} = \omega D(t) + \alpha S(t); \\ \frac{dD(t)}{dt} = \gamma I(t) - (\omega+\chi)D(t); \\ \frac{dX(t)}{dt} = \chi I(t) + \chi D(t); \\ \frac{dS(t)}{dt} + \frac{dI(t)}{dt} + \frac{dR(t)}{dt} + \frac{dD(t)}{dt} + \frac{dX(t)}{dt} = 0, \end{cases} \quad (1)$$

В качестве исходных параметров моделирования и сравнительной оценки были выбраны числовые значения характеристик процесса распространения компьютерных вирусов, характерные реальному функционированию ИТС локального уровня:

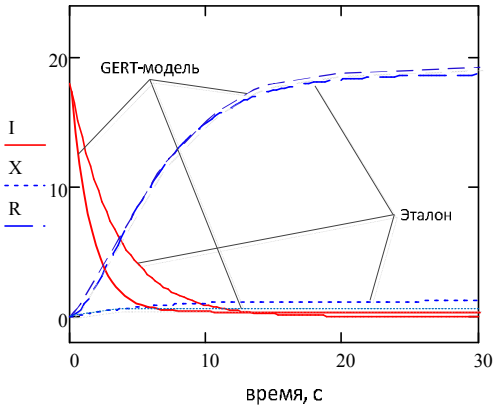
– α= 0,08; – γ= 0,3;

– ω= 0,3; – β= 0,2.

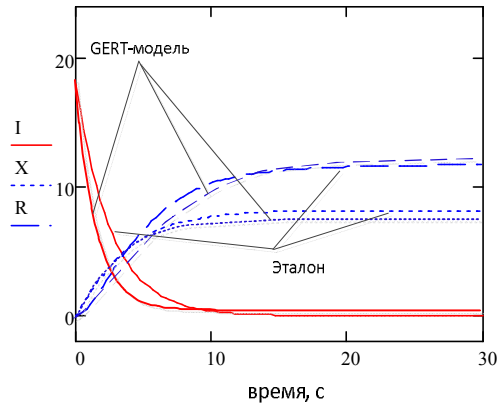
На рис. 4 представлены графики зависимости количества зараженных (I), выведенных из строя (X), и вылеченных (R) объектов от времени функционирования компьютерной системы, в различных начальных условиях зараженности сети.

Так, на рис. 4, а приводится семейство кривых, характеризующее перечисленные процессы в условиях, когда вероятность χ= 0,01, а уровень заражения ИТС на момент начала второй стадии $U = 1/N = 0,9$.

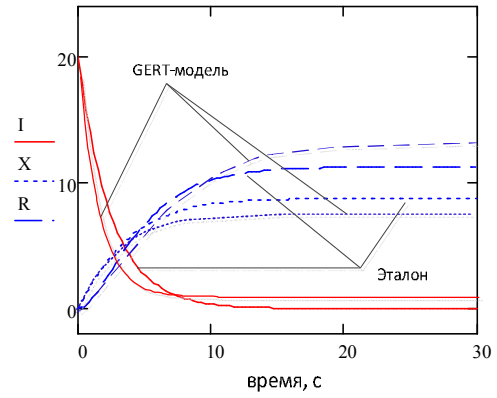
Аналогично на рис. 4, б определены следующие начальные условия: χ = 0,1, U=0,9; на рис. 4, в: χ = 0,1, U=1, на рис. 4, г: χ = 0,01, U = 1.



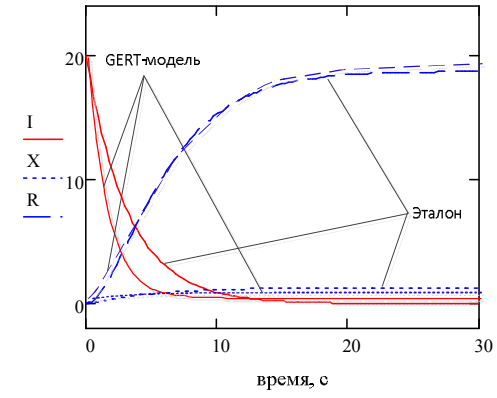
а



б



в



г

Рис. 4. Графики зависимости количества зараженных (I), выведенных из строя (X), и вылеченных (обладающих иммунитетом (R)) объектов от времени функционирования информационно-телекоммуникационной сети

Как видно из рисунка, в первом исследуемом случае (рис. 4, а), конечное количество выведенных из строя объектов $X \approx \{1,2\}$, во втором случае (рис. 4, б) это количество $X \approx \{7,8\}$, в третьем (рис. 4, в) – $X \approx \{8,9\}$, в четвертом (рис. 4, г) – $X \approx \{1,2\}$. Кроме этого, из рис. 4 видно, что учет в GERT-модели ключевой информации о состояниях телекоммуникационных узлов (интеллектуальных узлов коммутации) в процессе деструктивных воздействий компьютерных вирусов позволил повысить точность полученных результатов по сравнению с эталоном до 1,4 раза.

Выводы

Таким образом, проведены сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях. Описанная модель, в отличие от известных, учитывает ключевую информацию о состояниях телекоммуникационных узлов в процессе деструктивных воздействий компьютерных вирусов, а также фактор использования «облачного» антивирусного обеспечения в процессе лечения, что позволило повысить точность полученных результатов по сравнению с известными до 1,4 раза.

Список литературы

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

2. 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». Серія: Інформатика та моделювання. – Х.: НТУ «ХПІ», 2012. – Вип. 38. – С. 163-171.

3. Босько В.В. Математическая GERT-модель технологии передачи метаданных в облачные антивирусные системы / В.В. Босько, А.А. Смирнов, И.А. Березюк, Мохамад Абу Таам Гани // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 1(117). – С. 137-141.

4. Смирнов А.А. Структурно-логическая GERT-модель технологии распространения компьютерных вирусов / А.А. Смирнов, И.А. Березюк, Мохамад Абу Таам Гани // Системи управління, навігації та зв'язку. – П.: ПНТУ, 2014. – Вип. 1(29) .– С. 120-125.

5. Smirnov A.A. Experimental studies of the statistical properties of network traffic based on the BDS-statistics / A.A. Smirnov, D.A. Danilenko // International Journal of Computational Engineering Research (IJCER). – India. Delhi. – 2014. – Volume 4, Issue 5. – P. 41-51.

6. Кузнецов А.А. Дисперсионный анализ сетевого трафика для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях / А.А. Кузнецов, А.А. Смирнов, Д.А. Даниленко // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 2(118). – С. 124-133.

7. Matrosov A. Stuxnet under microscope. [Электронный ресурс] / A. Matrosov, E. Rodionov, D. Harley. – Режим доступа к ресурсу: http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf (Последний доступ 16 декабря 2012).

8. Cobb S. Stuxnet, Flamer, Flame, Whatever Name: There's just no good malware. [Электронный ресурс] / S. Cobb. – Режим доступа к ресурсу: http://blog.eset.com/2012/06/03/stuxnet-flamer-flame-whatever-name-there-is-no-good-malware (Последний доступ 16 декабря 2012).

9. Zesheng Chen. Modeling the spread of active worms. INFOCOM 2003. [Электронный ресурс] / Zesheng Chen, Lixin Gao, Kevin Kwait. – Режим доступа к ресурсу: http://www.ieee-infocom.org/2003/papers/46_03.PDF (Последний доступ 16 декабря 2012).

10. Williamson M.M. Epidemiological model of virus spread and cleanup. HPL-2003-39. [Электронный ресурс] / M.M. Williamson, J. Leveille. – Режим доступа к ресурсу: http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf (последний доступ 16 декабря 2012).

Поступила в редколлегию 7.10.2014

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Национальный технический университет «ХПИ», Харьков.

ПОРІВНЯЛЬНІ ДОСЛІДЖЕННЯ МАТЕМАТИЧНИХ МОДЕЛЕЙ ТЕХНОЛОГІЇ РОЗПОВСЮДЖЕННЯ КОМП'ЮТЕРНИХ ВІРУСІВ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Мохамад Абу Таам Гані, О.А. Смірнов, О.В. Коваленко, С.А. Смірнов

Проведено порівняльні дослідження математичних моделей технології поширення комп'ютерних вірусів в інформаційно-телекомунікаційних мережах. Описана модель, на відміну від відомих, враховує ключову інформацію про стани телекомунікаційних вузлів в процесі деструктивних впливів комп'ютерних вірусів, а також фактор використання «хмарного» антивірусного забезпечення в процесі лікування, що дозволило підвищити точність отриманих результатів у порівнянні з відомими до 1,4 разів.

Ключові слова: *інформаційно-телекомунікаційні мережі, комп'ютерні віруси, хмарні антивіруси, GERT-модель, математична модель PSIDDR.*

COMPARATIVE STUDY OF MATHEMATICAL MODELS OF TECHNOLOGY SPREAD OF COMPUTER VIRUSES IN THE INFORMATION AND TELECOMMUNICATIONS NETWORKS

Mohamad Abou Taam, A.A. Smirnov, A.V. Kovalenko, S.A. Smirnov

A comparative study of mathematical models of the spread of computer viruses technology in information and telecommunications networks. The model described, in contrast to the known, includes key status information telecommunication nodes in the destructive effects of computer viruses, as well as the factor of use "cloud" anti-virus software in the course of treatment that will improve the accuracy of the results obtained compared with the known 1, 4 times.

Keywords: *information and communication networks, computer viruses, cloud antivirus, GERT-model, mathematical model PSIDDR.*