ИССЛЕДОВАНИЕ ЖЕСТКОЙ МОДЕЛИ ДИНАМИКИ РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ В КРУПНОМАСШТАБНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Л.М. Груздева (Москва)

В исследовании динамики распространения вредоносных программ (ВП) в компьютерных сетях, в которых происходит два противоборствующих подпроцесса атаки и защиты субъектов сети, нашли широкое применение претерпевшие различные модификации эпидемиологические математические модели [1, 2, 3 и др.]. Наиболее релевантной для подобных исследований является SIR-модель Кермака-Маккендрика. Она базируется на предположении, что во время эпидемии некоторое количество заражённых субъектов либо избавляется от ВП, либо перестаёт функционировать. Как только субъект избавляется от вредоносной программы, он приобретает к ней иммунитет. Результаты исследований данной модели позволяют сделать вывод, что она не дает нужной точности в связи с тем, что в модели не учитываются топологические особенности крупномасштабной сети.

В [4] предложена новая модификация SIR-модели с учетом топологической уязвимости сети:

$$\begin{cases} \dfrac{dS(t)}{dt} = -2\ln\varphi\cdot\beta\cdot\dfrac{S(t)\cdot I(t)}{K} \\ \dfrac{dI(t)}{dt} = 2\ln\varphi\cdot\beta\cdot\dfrac{S(t)\cdot I(t)}{K} \\ \dfrac{dR(t)}{dt} = \gamma\cdot I(t) \end{cases} \quad (1)$$

Здесь $S(t)$ – число субъектов подверженных заражению, $I(t)$ – число разносчиков ВП, $R(t)$ – число восстановленных и имеющих защиту, K – общее количество субъектов $(K= S(t) + I(t) +R(t))$, γ – коэффициент восстановления/смерти, β – скорость заражения, φ - параметр топологической уязвимости сети, t – время.

Прогноз распространения ВП в крупномасштабной сети ($K=10^5..10^8$) может быть получен, например, с помощью системы автоматизированного проектирования MathCad, которая обладает мощным инструментарием для решения дифференциальных уравнений различного порядка. Одним из главных вопросов при выборе того или иного метода исследования системы (1) является точность приближенных значений и устойчивость получаемого решения.

Однако даже строго устойчивые методы могут вести себя неустойчиво, если шаг слишком велик. И хотя, в принципе, эту трудность можно преодолеть за счет уменьшения величины шага, это может привести к недопустимо большим затратам машинного времени. Такая ситуация возникает при решении дифференциальных уравнений, которые называются *жесткими*.

Система дифференциальных уравнений, записанная в матричной форме $y = A\cdot x$, где A – почти вырожденная матрица, называется жесткой. Решение таких систем характерно резко различной скоростью изменения значений переменных и требует очень малого шага, выбираемого исходя из наивысшей скорости изменения значений переменных. Одношаговые численные методы, в том числе метод Рунге-Кутта 4-го порядка, дают недопустимо большую ошибку при решении таких задач.

Для решения жестких дифференциальных уравнений рекомендуется использовать многошаговые методы, например неявные методы Адамса-Муолтона и явные методы Адамса-Башфорта. Причем, на практике рационально применять совместно явную и неявную формулы.

Перепишем систему (1) на языке MathCad:

$$\begin{cases} y'_0 = -2\ln(\varphi)\cdot\beta\cdot\dfrac{y_0\cdot y_1}{K} \\ y'_1 = 2\ln(\varphi)\cdot\beta\cdot\dfrac{y_0\cdot y_1}{K} \\ y'_2 = \gamma\cdot y_1 \end{cases} \quad (2)$$

Для сравнения используем две встроенные функции:

– Stiffb(y, x1, x2, npoints, D, J) – возвращает матрицу решений жесткого дифференциального уравнения, записанного в векторе D и функции Якобиана J, y – вектор начальных значений на интервале [x1, x2] (для решения используется метод Булирша-Штера);

– Stiffr(y, x1, x2, npoints, D, J) – для решения используется метод Розенброка.

Матрица-функции Якоби (якобиан) J имеет размер $n \times (n+1)$, первый столбец которой содержит частные производные *d**D**/dx*, остальные столбцы и строки представляют собой матрицу Якоби *d**D**/dyk* :

$$J(x,y) := \begin{pmatrix} 0 & -2\ln(\varphi)\cdot\beta\cdot\frac{y_1}{K} & -2\ln(\varphi)\cdot\beta\cdot\frac{y_0}{K} & 0 \\ 0 & 2\ln(\varphi)\cdot\beta\cdot\frac{y_1}{K} & 2\ln(\varphi)\cdot\beta\cdot\frac{y_0}{K}-\gamma & 0 \\ 0 & 0 & \gamma & 0 \end{pmatrix} \quad (3)$$

Чем более вырожденной является матрица Якоби, тем жестче система уравнений. Определитель матрицы Якоби (3) равен нулю при любых значениях y_0, y_1 и y_2:

$$\left| \begin{pmatrix} -2\ln(\varphi)\cdot\beta\cdot\frac{y_1}{K} & -2\ln(\varphi)\cdot\beta\cdot\frac{y_0}{K} & 0 \\ 2\ln(\varphi)\cdot\beta\cdot\frac{y_1}{K} & 2\ln(\varphi)\cdot\beta\cdot\frac{y_0}{K}-\gamma & 0 \\ 0 & \gamma & 0 \end{pmatrix} \right| \to 0 \quad (4)$$

Жесткость SIR-модели уже была снижена «вручную» с помощью масштабирования (слагаемые системы разделили на общее количество субъектов сети).

Как видно из рис. 1, обе функции дают одинаковое решение, при чем, необходимая точность прогноза пика эпидемии была получена уже при малом количестве шагов численных методов.

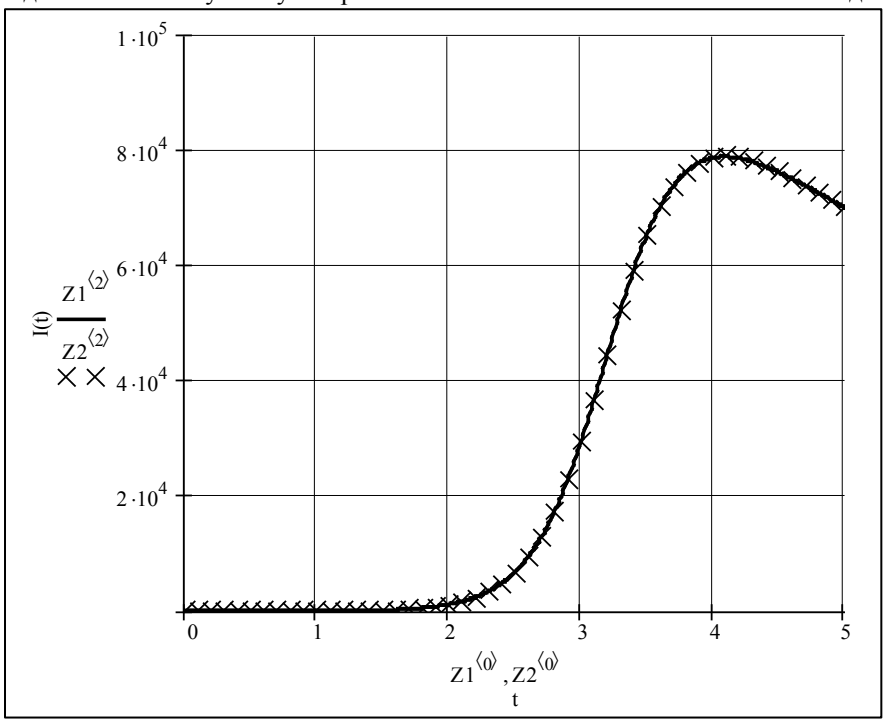

Рис. 1. Число ВП в сети разносчиков (K=10^5, I_0=1, β=0.3, γ =0.2, φ=530, R_0 =0)

На рис. 2 представлено решение, полученное методом Булирша-Штера.

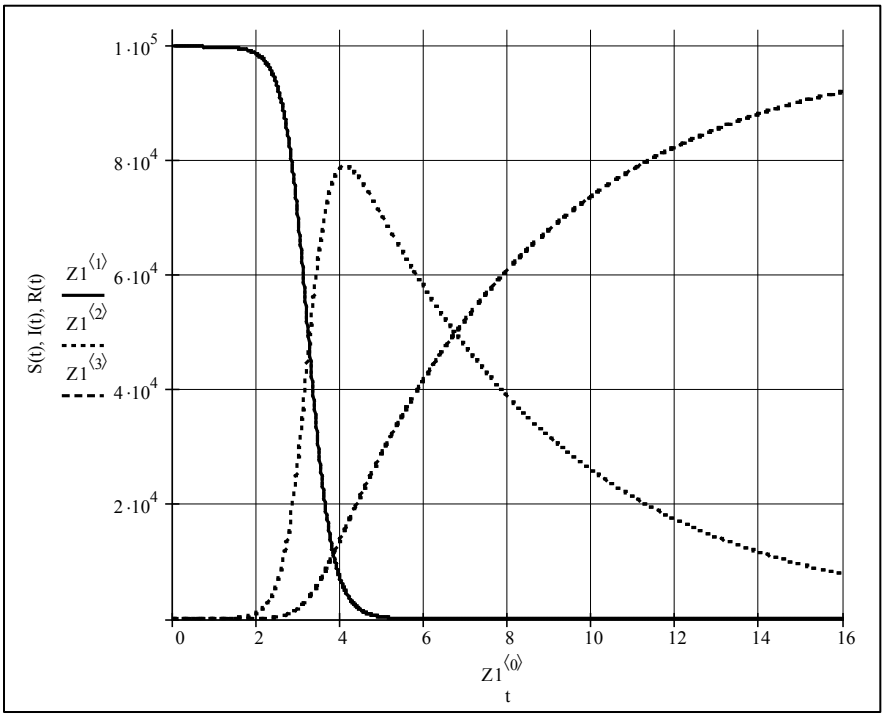

Рис. 2. Результаты тестирования SIR-модели (K=10^5, I_0=1, β=0.3, γ =0,2, φ=530, R_0 =0)

Проиллюстрируем влияние различных параметров, учтенных в модели, на процесс распространения вредоносных программ в сети. Коэффициент топологической уязвимости φ имеет большое влияние на длительность процесса и масштаб заражения субъектов сети (рис. 3).

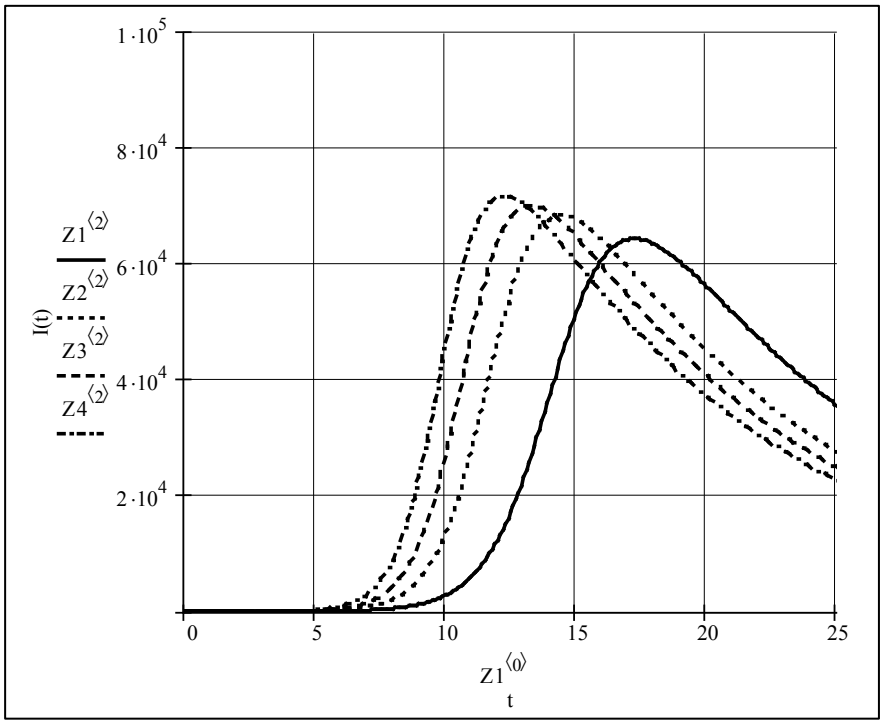

Рис. 3. Влияние φ на процесс распространение ВП (K=10^5, I_0=1, β=0,1, γ =0,1, R_0 =0, $Z1^{<2>}$ при φ=90, $Z2^{<2>}$ при φ=210, $Z3^{<2>}$ при φ=330, $Z4^{<2>}$ при φ=530)

Подпроцесс защиты зависит от начального количества защищенных субъектов сети R_0 и

коэффициента восстановления (вероятности защиты) γ.

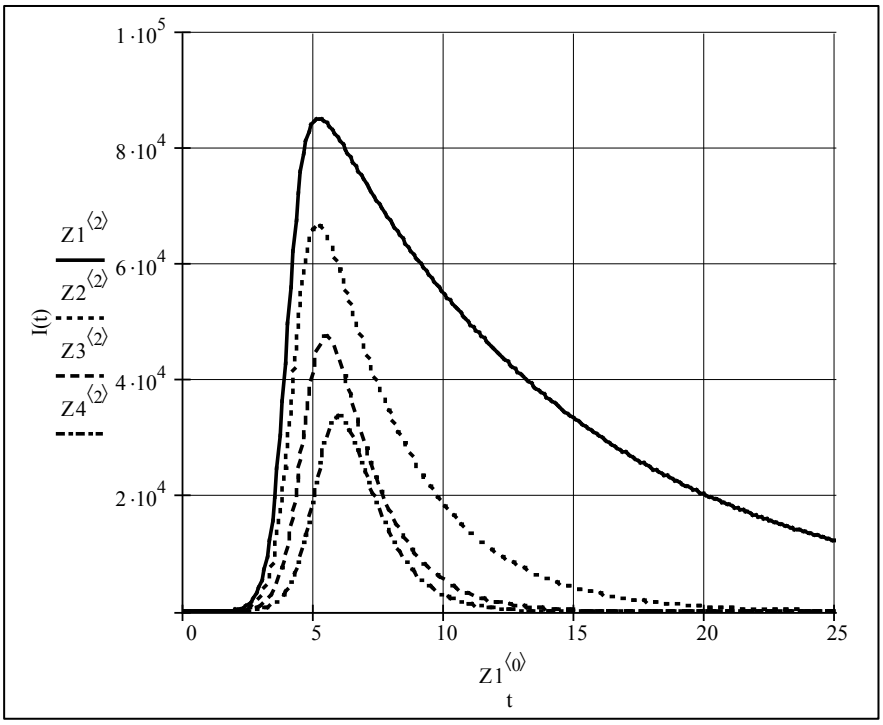

Рис. 4. Влияние γ на процесс распространение ВП (K=10^5, I_0=1, β=0.5, φ = 20, R_0 =0, $Z1^{<2>}$ при γ =0.1, $Z2^{<2>}$ при γ =0.3, $Z3^{<2>}$ при γ =0.6, $Z4^{<2>}$ при γ =0.9)

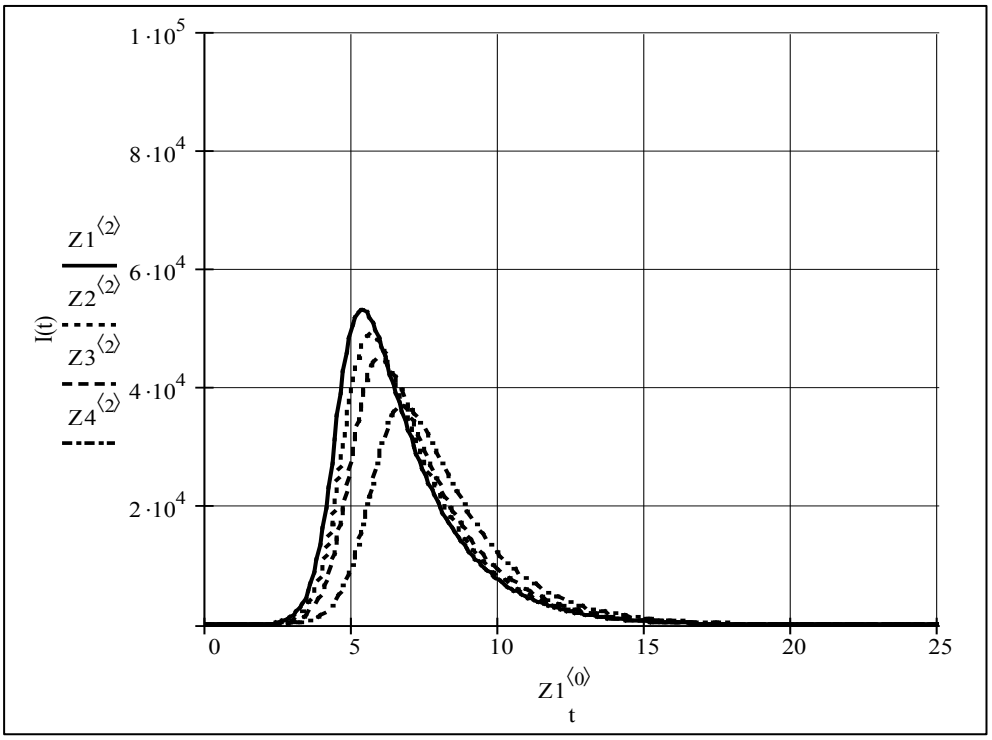

Рис. 5. Влияние $R0$ на процесс распространение ВП (K=10^5, I_0=1, β=0.5, φ = 20, γ =0,5, $Z1^{<2>}$ при R_0 =0, $Z2^{<2>}$ при R_0 =5000, $Z3^{<2>}$ при R_0 =10000, $Z4^{<2>}$ при R_0 =20000)

По результатам исследований можно сделать следующие выводы: при небольших значениях вероятности защиты (γ<0,3) ВП заражает практически все субъекты сети (рис. 4), а при случайном

выборе изначально защищенных узлов картина процесса распространения практически не изменяется (рис. 5).

Литература

1. Leveille J. Epidemic Spreading in Technological Networks http://www.hpl.hp.com/techreports/2002/HPL-2002-287.pdf.
2. Груздева Л.М. Применение имитационного моделирования для исследования характеристик эпидемии в распределенной информационно-вычислительной системе и процесса восстановления системы // Сборник докладов пятой всероссийской научно-практической конференции ИММОД-2011. – Санкт-Петербург: Изд-во Центр технологии и судостроения. Т. 2. – С. 66-69.
3. Теоретическое и экспериментальное исследование распределенных телекоммуникационных систем в условиях воздействия вредоносных программ [Текст]: монография / Ю. М. Монахов, Л. М. Груздева; М-во образования и науки Российской Федерации, ФГБОУ ВПО "Владимирский гос. ун-т им. Александра Григорьевича и Николая Григорьевича Столетовых". - Владимир: ВлГУ, 2013. - 131 с.

Абрамов К.Г. Модели угрозы распространения запрещенной информации в информационно-телекоммуникационных сетях – Диссертация на соискание ученой степени к.т.н.. Владим. Гос.ун-т. – Владимир: Изд-во Владим. Гос. Ун-та, 2014.