Математическое моделирование распространения вирусов в компьютерной сети

Короткова Дарья Алексеевна,
Ульяновский государственный университет
студентка

Научный руководитель:
Андреев Александр Сергеевич,
профессор

Защита компьютеров и сетей от вирусов является одной из важных задач на сегодня в IT-области. Число вредоносного программного обеспечения постоянно растет, а создание современных методов защиты от нового вируса занимает достаточное количество времени. Это порождает глобальные сетевые эпидемии. Поэтому создание максимально защищенных систем от проникновения вредоносного кода является одним из актуальных направлений в научных исследованиях информационной безопасности.

Для разработки таких систем необходимо использовать теоретические исследования в области компьютерной безопасности, известные на данный момент. Это позволит выявить различные свойства и факторы, влияющие на распространение вируса. Одним из исследований является математическое моделирование.

В данной статье изучается, наиболее приближенная к реальным условиям, математическая модель распространения вирусов PSIDR.

Ключевые слова: математическое моделирование, PSIDR, запаздывание.

Основной этап моделирования эпидемии вредоносных программ — выбор эпидемиологической модели, адекватно описывающей этот процесс. Большинство исследователей в области компьютерных вирусов проводят аналогию между вредоносным программным обеспечением и природными вирусами, сетевой эпидемией и биологической эпидемией.

С математической точки зрения органические и компьютерные вирусы имеют схожие характеристики и свойства, их распространение описывается сходными дифференциальными уравнениями. Исследование статистических данных также показывает адекватность применения модели эпидемии инфекционных заболеваний для описания процесса развития вирусной атаки. Поэтому использование теории математического моделирования биологических систем получило большое развитие в научных исследованиях по компьютерной безопасности.

В настоящее время известно несколько разновидностей математических моделей распространения компьютерных вирусов, которые отличаются между собой областью ограничения и условиями применения в реальных технических системах.

Среди них можно выделить следующие модели: SI, SIR, AAWP, PSIDR.

Модель SI характеризуется наличием двух типов объектов управления: зараженные (I) и не зараженные (S). Характерной особенностью SI модели является пренебрежение антивирусным ПО, что приводит к необратимости эпидемического процесса в компьютерных системах.

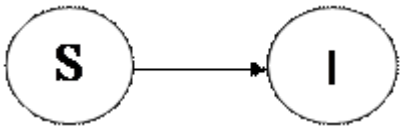


Рис 1. Граф состояний модели SI.

Формально, это означает, что вероятность успешного размножения вируса составит

$$P(t) = \frac{S(t)}{N} = 1 - \frac{I(t)}{N}, \text{где } N = S(t) + I(t)$$

Приращение количество вируса на бесконечно малом интервале

$\Delta I = I(t)\beta\left(1 - \frac{I(t)}{N}\right)\Delta t$, а дифференциальное уравнение, которое описывает динамику эпидемий, будет выглядеть так:

$$\frac{dI(t)}{dt} = \frac{\beta I(t) - \beta I(t)^2}{N} = \frac{\beta I(t) S(t)}{N}$$

Решение этого уравнения записывается следующим образом:

$$I(t) = \frac{1}{\frac{1}{N} + \frac{1}{\beta}\exp(-\beta(t + C))}$$

Константа $C = -\frac{1}{\beta}\ln(\frac{\beta}{I_0} - \frac{\beta}{N})$ учитывает начальное условие $I(0) = I_0$.

График функции I(t) на начальном этапе ведет себя, как экспонента, но затем замедляет свой рост и стремится к асимптоте N.

В связи с отсутствием антивируса, который влияет на процесс распространения компьютерных вирусов, эпидемия не может угаснуть. Кривые зависимости изменения количества зараженных узлов от времени функционирования компьютерной системы в условиях распространения эпидемии по модели SI при разных коэффициентах заражения b представлены на рис. 2.

Анализ графиков показал, что коэффициент заражения b прямопропорционально влияет на скорость распространения вируса.

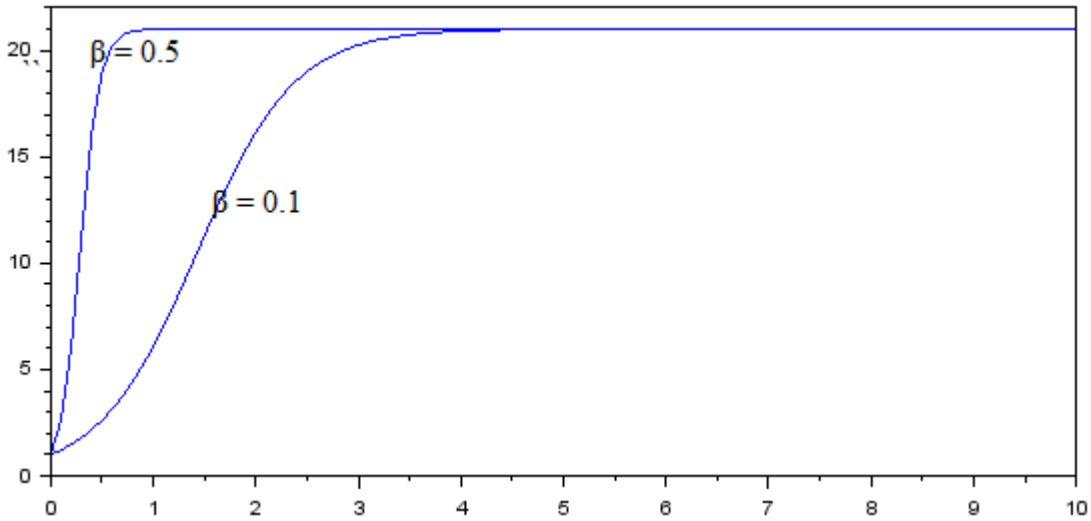


Рис 2. Количество зараженных субъектов в модели SI.

Модель PSIDR (Progressive Susceptible—Infected—Detected—Removed model) характеризуется наличием четырех состояний: зараженные (I), не зараженные (S), найденные зараженные объекты (D), вылеченные объекты, обладающие иммунитетом ®. Поведение системы, описанное с помощью модели PSIDR, делится на два этапа:

Период свободного распространения вируса в сети.

Вирус распространяется согласно SI модели в течение некоторого времени со скоростью β.

Период обнаружения вредоносного ПО.

В этой фазе скорость распространения остается прежней, восприимчивые субъекты вакцинируются со скоростью μ, а инфицированные обнаруживаются со скоростью μ и «лечатся» со скоростью δ.

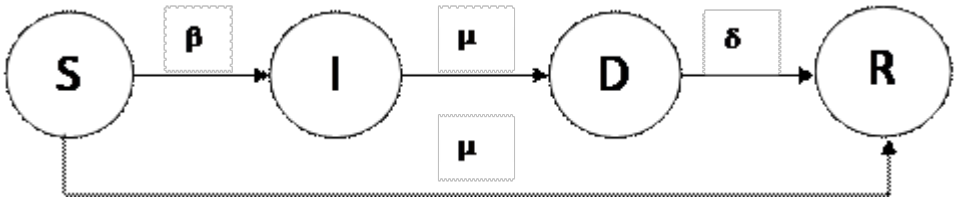


Рис 3. Граф состояний второго этапа PSIDR.

Модель распространения вирусов в компьютерной сети PSIDR, позволяет оценить динамику изменения количества уязвимых, зараженных, найденных и имеющих иммунитет субъектов, и может быть записана с помощью системы дифференциальных уравнений с запаздыванием:

$$\begin{cases} \frac{dS(t)}{dt} = -\beta S(t)I(t) \\ \frac{dI(t)}{dt} = \beta S(t)I(t) \\ N = S(t) + I(t) \end{cases}$$

$$\begin{cases} \frac{dS(t)}{dt} = -\beta S(t)I(t) - \mu S(t) \\ \frac{dI(t)}{dt} = \beta S(t)I(t) - \mu I(t) \\ \frac{dD(t)}{dt} = \mu I(t) - \delta D(t-h) \\ \frac{dR(t)}{dt} = \delta D(t-h) + \mu S(t) \\ N = I(t) + S(t) + R(t) + D(t) \end{cases}$$

где b — частота заражения; d — частота лечения; m — вероятность вылечивания, S(t) — количество уязвимых объектов; I(t) — количество зараженных объектов; R(t) — количество вылеченных (с иммунитетом) объектов (на первой стадии = 0); D(t) — количество обнаруженных зараженных объектов (на первой стадии = 0).

Кривая зависимости изменения обнаруженных узлов от времени функционирования компьютерной системы по модели PSIDR представлена на рис. 4.

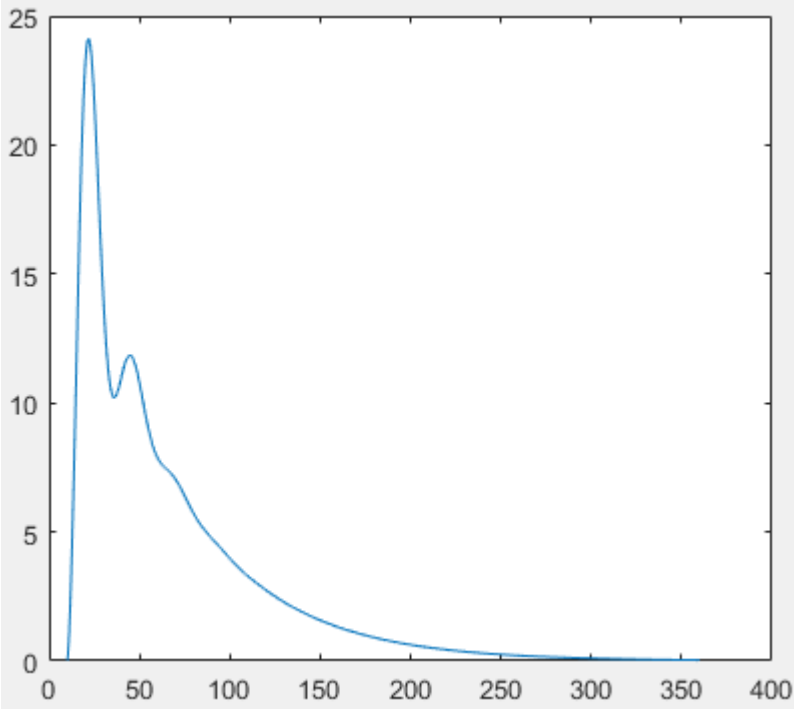


Рис 4. График зависимости обнаруженных зараженных компьютеров от времени в модели PSIDR.

Количество обнаруженных зараженных объектов $D(t)$ стремится к нулю. Решения могут иметь как характер затухающих колебаний (рис. 5), так и апериодический характер (рис. 6). Всё зависит от параметра запаздывания.

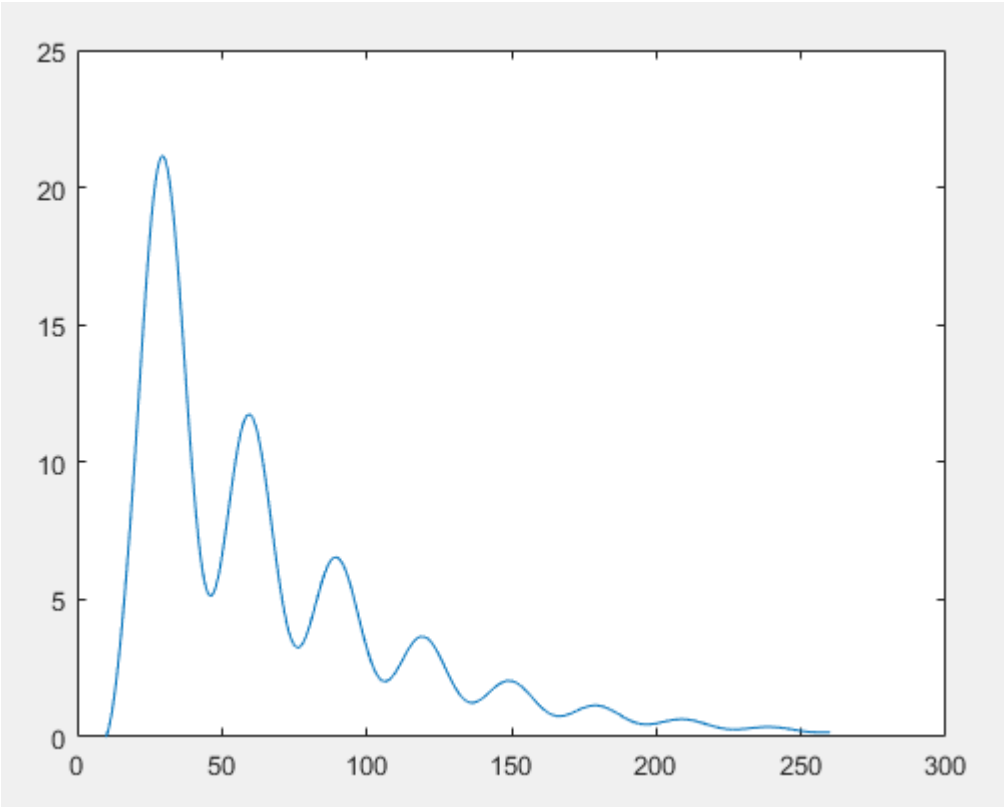


Рис 5. График зависимости обнаруженных зараженных компьютеров от времени в модели PSIDR с h = 1.

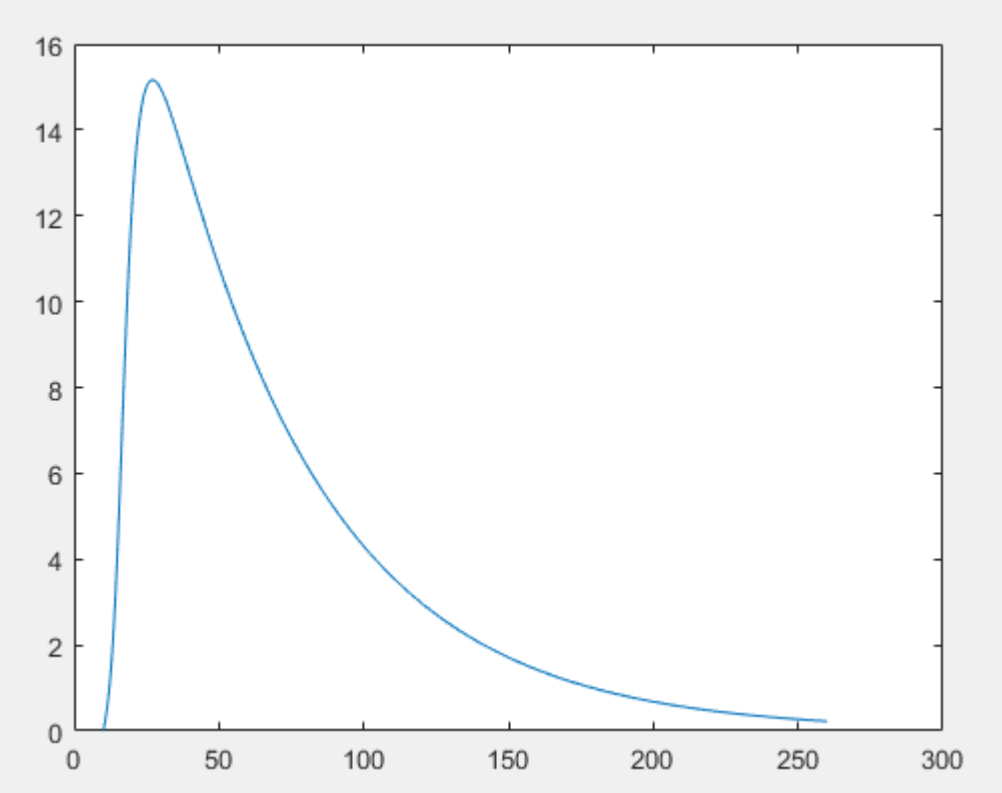


Рис 6. График зависимости обнаруженных зараженных компьютеров от времени в модели PSIDR c h = 0.1.

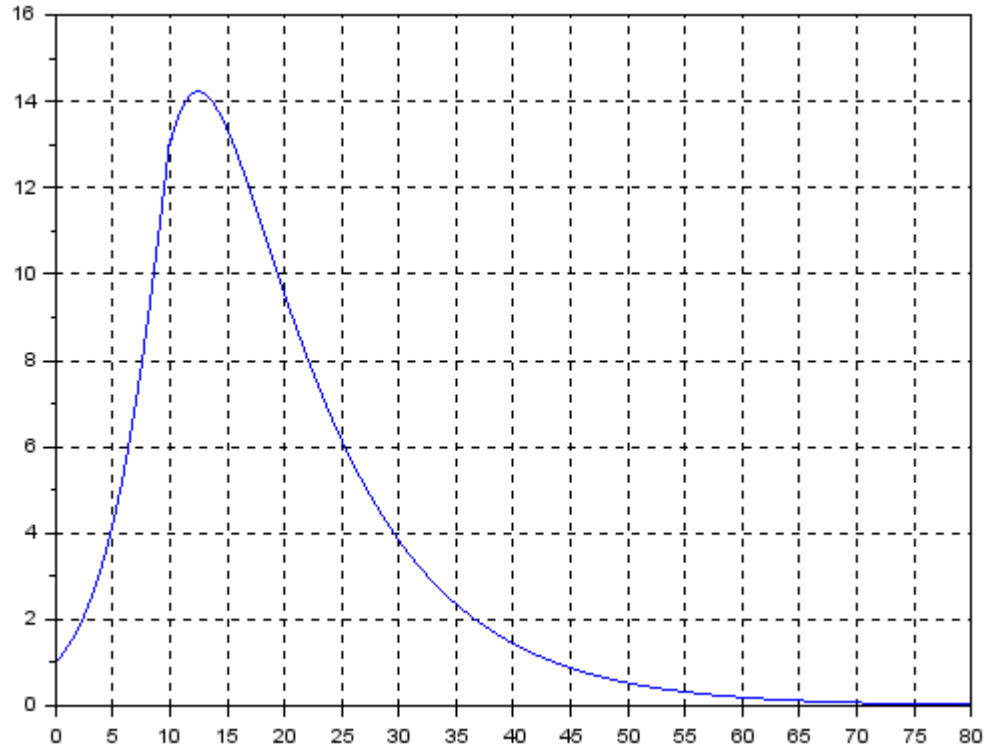


Рис 7. График зависимости инфицированных субъектов

от времени в модели PSIDR.

Проведенный анализ модели PSIDR показал, что она является наиболее подробной, так как разбиение модели распространения компьютерных угроз на два этапа дает возможность независимого анализа процесса заражения и лечения, а введение запаздывания может быть обусловлено «немгновенной» реакцией антивируса на инфицированные субъекты.

Литература

1. Котенко И.В. Аналитические модели распростра- нения сетевых червей / И.В. Котенко, В.В. Воронцов // Труды СПИИРАН. — СПб.: Наука, 2007. — Вып. 4.
2. Williamson M. Epidemiological model of virus spread and cleanup [Электронный ресурс] / M. Williamson, J. Leveille // HP Laboratories Bristol (February 27th, 2003).
3. Столингс, В. Основы защиты сетей. Приложения и стандар- ты / В. Столлингс. — М. : Вильямс, 2002. — 432 с. — ISBN 5-8459-0298-3.
4. Daley, D.J. and Gani, J. Epidemic Modeling: An Introduction. Cambridge University Press, 1999.