УДК 681.3.06

*А.А. ЗАХАРЧЕНКО, М.А. ХАЖМУРАДОВ*

# ДИНАМИКА СЕТЕВЫХ ЭПИДЕМИЙ И ЭФФЕКТИВНОСТЬ СИСТЕМ ЗАЩИТЫ

Рассматривается динамика распространения компьютерных сетевых червей на основе классических эпидемиологических моделей (SIS и SIR). Определяются характерные фазы развития сетевой эпидемии и выбираются критерии эффективности систем защиты сетей от проникновения вирусов.

## 1. Введение

Со времени первой глобальной эпидемии червя Морриса [1] распространение сетевых червей-вирусов представляет собой основную проблему компьютерной безопасности. Представители этого класса злонамеренных саморазмножающихся программ используют уязвимости и ошибки реализации широко распространенных сетевых сервисов. Несмотря на существенный прогресс в области разработки антивирусного программного обеспечения (ПО), большинство антивирусов не способны уверенно детектировать новый саморазмножающийся программный код до внесения его сигнатур в антивирусные базы. Вследствие этого в глобальных сетях периодически возникают эпидемии распространения вирусов, охватывающие одновременно десятки стран.

Математический аппарат для изучения динамики «обычных» биологических эпидемий был разработан достаточно давно [2]. Биологический подход к моделированию вирусной проблемы [3] начался с работ J.O. Kephart и S.R. White из IBM [4], однако актуальным это направление стало в 2001 г. после эпидемических вспышек сетевых червей Code Red и Nimda [5]. Значительный резонанс получили работы N. Weaver, в которых введена концепция Warhol (или блицкриг) червей, а также исследованы различные концептуальные алгоритмы размножения самовоспроизводящихся кодов, кардинально повышающие эффективность их распространения [6, 7].

*Цель* данного исследования состоит в анализе классических моделей распространения сетевых червей и установлении на их основе общих подходов к оценке эффективности защиты сетей от проникновения вирусов.

## 2. Простая эпидемическая модель (SIS-модель)

Рассмотрим простую эпидемическую модель, в которой предполагается, что произвольный узел сети, состоящей из постоянного количества (N) компьютеров, может находиться только в двух состояниях: уязвимом (S) и инфицированном (I), S + I = N. Предположим, что на каждом инфицированном узле может существовать только одна копия червя, которая случайным образом выбирает в доступном адресном пространстве потенциальную жертву со средней постоянной скоростью $\beta$ (на поиск и заражение одного узла в среднем тратится $1/\beta$ секунд). В первом приближении $\beta$ определяется средней скоростью сканирования червем сети ($V_S$) и размером её адресного пространства ($N_{ip}$):

$$\text{в} = V_s \times \frac{N}{N_{ip}}.$$

Динамика количества инфицированных узлов в такой сети описывается уравнением

$$\frac{di}{dt} = \text{в}(1-i)i, \qquad (1)$$

где i = I/N – доля инфицированных узлов в сети. Доля уязвимых узлов s=S/N связана с долей инфицированных узлов i через соотношение s = 1–i.

Предполагая, что в начальный момент времени $t_0 = 0$ доля инфицированных узлов составляет $i_0$, получаем

$$i(t) = \frac{1}{1 + \left[\frac{1}{i_0} - 1\right]\exp(-\beta t)}. \qquad (2)$$

Таким образом, распространение червей в рассматриваемой модели полностью определяется двумя параметрами: скоростью размножения червя ($\beta$) и начальной инфицированностью рассматриваемой сети ($i_0$).

Из приведенных в [6] данных следует, что для Code Red (v2) $i_0 \sim 10^{-11}\ldots10^{-10}$, т. е. можно предполагать, что червь начинал атаку на Интернет с одного компьютера.

Динамика функции (2) характеризуется тремя четко различимыми этапами (рис. 1).

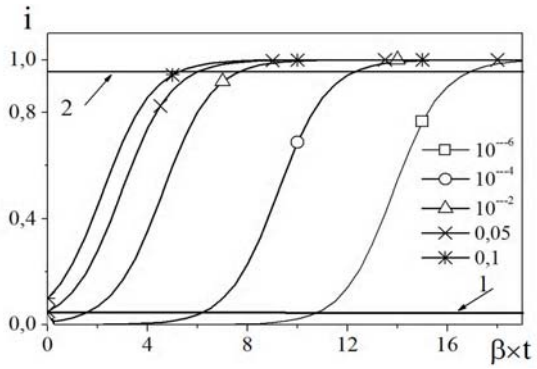


Рис. 1. Развитие эпидемии в зависимости от начальной зараженности сети

Первый этап – сравнительно медленное (но тем не менее экспоненциальное) нарастание зараженности сети до порогового уровня $i_{пор} \approx 0{,}05$ (прямая 1 на рис. 1). Скорость удвоения доли пораженных машин на этом этапе равна $\ln(2)/\beta$.

Второй этап – взрывная фаза (outbreak) в диапазоне $0{,}05 < i < 0{,}95$. Продолжительность её определяется только скоростью инфицирования $\beta$ и приблизительно равна $5{,}89/\beta$.

Третий этап – насыщение, $i > 0{,}95$ (прямая 2 на рис. 1). На этом участке при случайном сканировании адресного пространства зараженные узлы контактируют преимущественно друг с другом, поэтому уцелевшие узлы могут оставаться «чистыми» неопределенное время.

Для достижения порога насыщения $i_{пор}$ =0,95 требуется время

$$\frac{1}{в}\ln\left[19\left(\frac{1}{i_0} - 1\right)\right],$$

из чего следует, что в пределах применимости рассматриваемой модели динамика эпидемии не зависит от масштабов сети. К примеру, сеть из миллиона уязвимых компьютеров, в которой в начальный момент времени инфицирован только один узел, будет практически полностью заражена за то же время, что и аналогичная сеть из ста миллионов компьютеров, где в начальный момент окажется всего 100 инфицированных узлов.

Механизм случайного выбора жертвы ограничивает снизу скорость распространения вирусов по сети. Значительно повысить её можно достаточно простыми средствами: подготовкой предварительного списка адресов для атаки, сканированием подсетей, выделением каждой копии червя отдельного фрагмента сетевого адресного пространства, поиском подходящих мишеней на зараженном компьютере и др. [6]. Например, если копия червя получает «в наследство» только половину адресного пространства от «родителя», то это эквивалентно удвоению скорости заражения каждые $1/\beta$ единиц времени с каждым циклом размножения червя (рис. 2).

Инфекционная способность $\beta$ в значительной степени зависит от скорости прохождения сетевых пакетов. В настоящее время все большее распространение получает широкополосный доступ к Интернет, связанный с необходимостью массовой передачи потоков видеоинформации, что автоматически повышает скорость распространения червей.

Системы раннего оповещения о развитии эпидемии окажутся эффективными только на участке $i \ll i_{пор}$ и при крайне низких значениях скорости размножения $\beta$. Моделирование распространения

червей Code Red и Slammer [8] показало, что анализ обращений к несуществующим адресам позволяет определить признаки вирусной активности в сети при заражении 1–2 % уязвимых узлов [9]. Таким образом, предупреждение может быть получено максимум за $1{,}65/\beta$ секунд до достижения порога взрыва $i_{пор}$. Согласно данным [9] в случае Code Red это время составило бы не более 50 минут, а для Slammer не превысило бы 15–20 секунд. Очевидно, что в обоих случаях эпидемии можно было бы только зафиксировать, но не предотвратить.

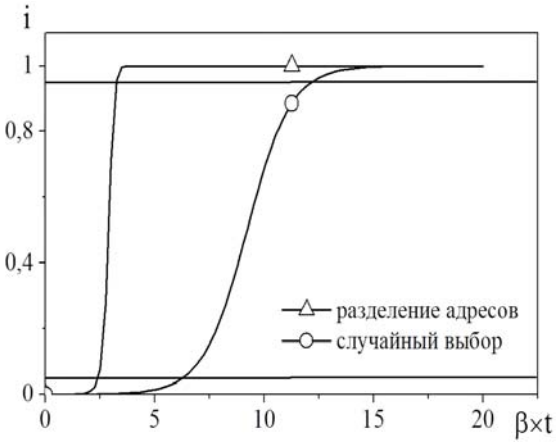

Рис. 2. Ускорение эпидемии при выделении каждой копии червя отдельного фрагмента адресного пространства

Эффективность сетевых эпидемий можно значительно повысить, проводя скрытное предварительное заражение отдельных уязвимых узлов. Чем ближе $i_0$ к $i_{пор}$, тем разрушительнее могут оказаться последствия вирусной атаки (см. рис. 1).

Анализ эпидемий Code Red v2 и Slammer на основе простой модели показал удовлетворительное совпадение с реально наблюдаемой динамикой эпидемий. Уже Code Red v2, чья инфицирующая способность оценивалась по различным данным от 0,7 до 1,8 компьютера в час, менее чем за половину суток мог получить контроль над сотнями тысяч серверов. Slammer при скорости удвоения 8,5 секунд имел инфицирующую способность ~293 узлов в час и мог проникнуть на 90% уязвимых компьютеров всего лишь за 10 минут.

### 3. SIR модель и её варианты

Факторы, обеспечивающие затухание сетевых эпидемий, можно оценить на модели, в которой сетевые узлы существуют в трех состояниях: уязвимом (S), зараженном (I) и невосприимчивом к заражению (R): S + I + R = N. Для начала предположим, что узлы оказываются неуязвимыми после излечения от инфекции. Вводя постоянную среднюю скорость «иммунизации» в единицу времени $\gamma$, получаем систему уравнений:

$$\begin{cases} \dfrac{ds}{dt} = -\beta is, \\ \dfrac{di}{dt} = \beta is - \gamma i, \\ \dfrac{dr}{dt} = \gamma i, \end{cases} \qquad (3)$$

где r = R/N - доля неуязвимых узлов и s + i + r = 1.

В этой модели существует пороговое условие для развития эпидемии [2]. На участке возрастания i(t) производная di/dt должна быть больше 0. Поскольку s(t) непрерывно уменьшается за счет инфицированных машин, то получаем, что для начала эпидемии необходимо, чтобы доля уязвимых узлов в начальный момент времени была

$$s(0) > \gamma/\beta. \qquad (4)$$

Данное условие выполняется практически всегда, поскольку значение $\gamma$ определяется запаздывающей человеческой реакцией и необходимостью загрузки громоздких «заплат» для ПО, а $\beta$ – постоянно улучшающимися техническими характеристиками сети и «доброй волей» злоумышленника (он может вставить небольшую паузу в цикл размножения, чтобы не создавать катастрофического трафика и слегка понизить скорость инфицирования). Доля же уязвимых узлов в реальных сетях обычно очень велика. Поэтому $\beta$ на много порядков превосходит $\gamma$. (К примеру, при моделировании эпидемии Code Red v2 [10] согласие с реальными данными достигнуто при соотношении $\beta/\gamma \sim 10^6$.)

В реальных условиях «иммунитет» посредством установки антивирусного ПО, межсетевых экранов и «заплат» приобретают не только инфицированные узлы (I), но и уязвимые (S). Предполагая, что средняя скорость иммунизации примерно одинакова для узлов обоих типов и равна величине $\gamma$, получаем:

$$\begin{cases} \dfrac{di}{dt} = \beta i(1 - r - i) - \gamma i, \\ \dfrac{dr}{dt} = \gamma(1 - r). \end{cases} \qquad (5)$$

Условие (4) для развития эпидемии в этой модели сохраняется.

Динамика доли неуязвимых узлов в системе (5) определяется уравнением

$$r(t) = 1 - \exp(-\gamma t),$$

откуда вытекает, что любую эпидемию теоретически можно преодолеть. Однако необходимое для этого время может оказаться неприемлемо большим (рис. 3, 4).

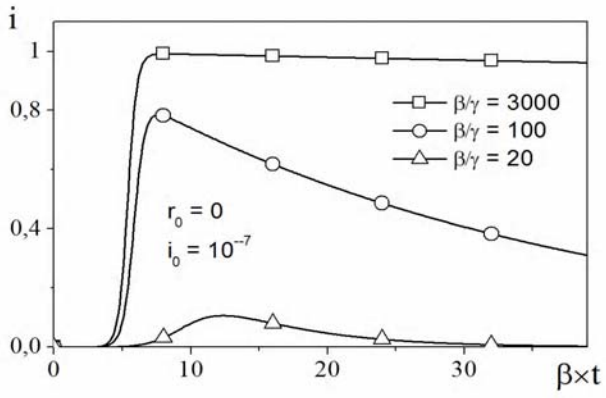


Рис. 3. Динамика развития эпидемии в системе при сравнительно малой начальной зараженности сети ($10^{-7}$). При $\beta/\gamma < 15$ вспышка не происходит

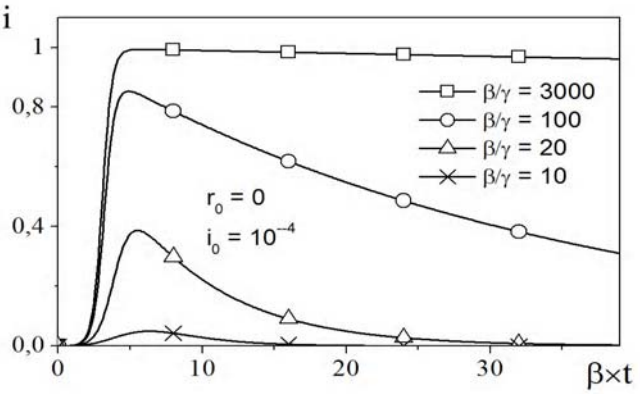


Рис. 4. Динамика развития эпидемии в системе при значительной начальной зараженности сети ($10^{-4}$). Пороговое значение вспышки $\beta/\gamma < 9$

Основной отличительной особенностью системы с приростом уязвимых узлов оказывается наличие постоянного уровня, к которому со временем стремиться доля инфицированных компьютеров (рис. 5).

Как показано в [11], динамика заражения системы с переменным числом узлов определяется скоростью прироста новых уязвимых узлов $\alpha$. Условие развития эпидемии в таких системах приобретает вид

$$s(0) > (\gamma + \alpha)/\beta.$$

Это означает, что в реальных условиях от конкретного вируса в системе с приростом уязвимых узлов полностью избавиться нельзя даже при автоматической «вакцинации». Хотя бы и незначительное постоянное добавление новых уязвимых узлов создает «резервации», которые в настоящее время обеспечивают функционирование и рост ботнетов – сетей, объединяющих компьютеры с программным обеспечением, выполняющим скрытые от владельцев задачи.

## 4. Выводы

1. Однородность глобальных сетей относительно определенной уязвимости представляет главную угрозу. Практика показала, что даже черви, которые выбирают жертву случайным образом и, следовательно, являются самыми медленными, за считанные минуты способны поразить ключевые узлы Интернета и вывести из строя телекоммуникации на уровне отдельных стран [8]. Таким образом, любая структура, деятельность которой критически зависит от бесперебойного функционирования сети, должна иметь резервные системы, построенные на программном обеспечении с различающимся кодом.

2. Архитектура сетей должна проектироваться таким образом, чтобы максимально понижать скорость инфицирования отдельных узлов в том случае, если злонамеренному коду удастся проникнуть в сеть. Экспоненциальный рост количества зараженных узлов в сети свидетельствует об отсутствии в ней защитных механизмов либо об их неэффективности. Например, в сетях с экспоненциальным ростом могут оказаться неэффективными системы раннего оповещения, основанные на выявлении запросов к несуществующим в данной сети адресам.

3. Для предотвращения эпидемических вспышек скорость устранения уязвимых компьютеров в сети должна быть не менее 15% от возможной скорости инфицирования отдельных узлов. В настоящее время этого соотношения достичь невозможно.

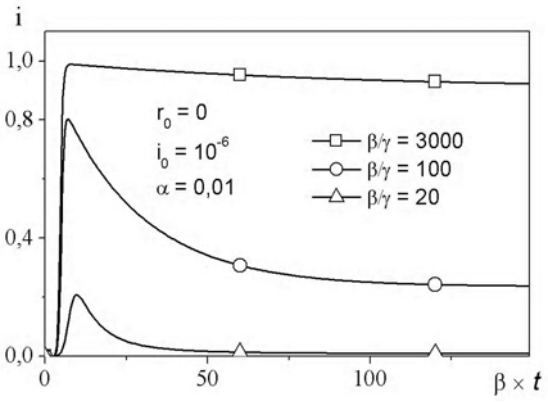


Рис. 5. Динамика развития эпидемии в сети с приростом уязвимых узлов

4. В растущих сетях с добавлением уязвимых узлов после ликвидации взрывной фазы вирусной вспышки доля инфицированных узлов стремится к постоянному уровню, что благоприятствует созданию и развитию бот-сетей.

**Список литературы:** 1. *Безруков Н.Н.* Компьютерная вирусология. Киев, УРЕ, 1991. 416 с. 2. *Hethcote H.W.* The Mathematics of Infectious Diseases // SIAM Review. 2000. V.42, No. 4. P. 599-653. 3. *Li J. and Knickerbocker P.* Functional similarities between computer worms and biological pathogens // Computers & Security. 2007. V. 26. P. 338-347. 4. *Kephart J.O. and White S.R.* Directed-Graph Epidemiological Models of Computer Viruses / Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy; Oakland, California, May 20-22. 1991. P. 343-359. 5. *Zou C.C., Gong W. and Towsley D.* Code Red Worm Propagation Modeling and Analysis / In 9th ACM Symposium on Computer and Communication Security, Washington DC. 2002. P. 138-147. 6. *Staniford S., Paxson V. and Weaver N.* How to Own the Internet in Your Spare Time / Proceedings of the 11th USENIX Security Symposium, 2002. P. 149-167. 7. *Weaver N.* Warhol Worms: The Potential for Very Fast Internet Plagues / http://www.cs.berkeley.edu/~nweaver/warhol.html. 8. *Moore D., Paxson V., Savage S. et al.* Inside the Slammer Worm // IEEE Security and Privacy. 2003. V. 1(4). P. 33-39. 9. *Zou C.C., Gao L., Gong W., Towsley D.* Monitoring and Early Warning for Internet Worms / Proc. CCS'03, October 27–30, 2003, Washington, DC, USA. P. 190-199. 10. *Chen Z., Gao L., Kwiat K.* Modeling the Spread of Active Worms // Proc. IEEE. INFOCOM, 2003. P. 1890–1900. 11. *Захарченко А.А.* Черводинамика: причины и следствия // Защита информации. Конфидент. 2004. № 2. С. 50-55.

*Поступила в редколлегию 12.06.2008*

**Захарченко Александр Алексеевич**, ведущий инженер-исследователь ННЦ ХФТИ. Научные интересы: физика и моделирование полупроводниковых детекторов ядерных излучений, черводинамика. Адрес: Украина, 61108, Харьков, ул. Академическая, 1, тел. 335-66-37. E-mail: az13@mail.ru

**Хажмурадов Манап Ахмадович**, д-р техн. наук, профессор, начальник отдела ННЦ ХФТИ. Научные интересы: математическое моделирование физических процессов и систем, автоматизация проектирования, программирование. Адрес: Украина, 61108, Харьков, ул. Академическая, 1, тел. 335-68-46. E-mail: khazhm@kipt.kharkov.ua