УДК 519.21 DOI: 10.32362/2500-316X-2019-7-3-7-27

Стохастические и перколяционные модели динамики блокировки вычислительных сетей при распространении эпидемий эволюционирующих компьютерных вирусов

С.А. Лесько[@],
А.С. Алёшкин,
В.В. Филатов

МИРЭА – Российский технологический университет, Москва 119454, Россия
[@]Автор для переписки, e-mail: sergey@testor.ru

В работе представлена комплексная модель динамики развития эпидемий вирусов в компьютерных сетях, созданная на основе учета их топологических свойств и механизмов распространения вирусов. С одной стороны, данная модель основана на использовании методов теории перколяции, которые позволяют определить такие структурно-информационные характеристики сетей, как зависимость порога перколяции от среднего числа связей (приходящихся) на один узел (плотность сети). С другой стороны, рассматриваются динамические процессы стохастического распространения в компьютерных сетях эволюционирующих вирусов при устаревании и запаздывании действия антивирусов. В работе рассматривается понятие порога перколяции, приводится уравнение зависимости величины порога перколяции сети от её плотности, полученное в результате анализа данных численного моделирования. Динамика распространения вирусов разработана с использованием двух подходов: первый основан на описании диаграмм переходов между состояниями узлов, после чего строится система кинетических дифференциальных уравнений распространения вирусов; второй – на рассмотрении вероятностей переходов между возможными состояниями всей сети в целом. Получено дифференциальное уравнение второго порядка и сформулирована краевая задача, решение которой описывает зависимость вероятности блокирования сети от вероятности блокирования отдельного узла. Это решение позволяет также оценить время достижения порога перколяции. В модель заложены эволюционные свойства вирусов (ранее иммунизированные или вылеченные узлы через некоторый интервал времени могут быть снова инфицированы), и время запаздывания антивирусной защиты. Анализ полученных решений для созданных моделей показывает возможность существования различных режимов распространения вирусов. Подчеркнуть, что при некоторых наборах величин коэффициентов дифференциальных уравнений наблюдается осциллирующий и почти периодический характер распространения вирусных эпидемий, что в значительной степени совпадает с реальными наблюдениями.

Ключевые слова: модель эволюционирующих компьютерных вирусов, осциллирующая динамика эпидемий компьютерных вирусов, времена запаздывания, диаграммы переходов между состояниями узлов, стохастические процессы, порог перколяции сетей со случайной структурой.

Stochastic and Percolating Models of Blocking Computer Networks Dynamics during Distribution of Epidemics of Evolutionary Computer Viruses

Sergey A. Lesko[@],
Anton S. Alyoshkin,
Vyacheslav V. Filatov

MIREA – Russian Technological University, Moscow 119454, Russia
[@]Corresponding author e-mail: mailto:sergey@testor.ru

The paper presents a complex model of the dynamics of virus epidemies propagation in computer networks, based on topological properties of computer networks and mechanisms of the viruses spread. On one hand, this model is based on the use of percolation theory methods, which makes it possible to determine such structural-information characteristics of networks as the dependence of the percolation threshold on the average number of connections per one node (network density). On the other hand, the dynamic processes of stochastic propagation in computer networks of evolving viruses are observed when anti-virus programs become outdated and postponed. The paper discusses the concept of percolation threshold, provides an equation for the dependence of the percolation threshold of a network on its density obtained by analyzing numerical simulation data. The dynamics of virus epidemies were studied through two approaches. The first one is based on the description of transition diagrams between states of nodes, after which a system of kinetic differential equations for the virus epidemies is constructed. The second is based on considering the probabilities of transitions between possible states of the entire network. A second-order differential equation is obtained in this article, and a boundary value problem is formulated. Its solution describes the dependence of the network blocking probability on the blocking probability of an individual node. The solution also makes it possible to estimate the time required to reach the percolation threshold. The model incorporates the evolutionary properties of viruses: previously immunized or disinfected nodes can be infected again after a certain time interval. Besides, the model incorporates a lag of the anti-virus protection. Analysis of the solutions obtained for the models created shows the possibility of various modes of virus propagation. Moreover, with some sets of values of differential equation coefficients, an oscillating and almost periodic nature of virus epidemies is observed, which largely coincides with real observations.

Keywords: computer model evolving viruses, oscillating dynamics of computer viruses epidemies, lag times, state transition graphs, stochastic processes, percolation threshold of networks with random topologies.

Введение

Развитие методов искусственного интеллекта уже сегодня позволяет создавать вирусы, которые могут эволюционировать и приспосабливаться к появлению новых антивирусных программ, что в значительной степени схоже с эволюцией биологических объектов. Не далек тот день, когда появится возможность автоматического создания в сетях новых вирусов, основанных на принципах эволюционного отбора и анализе те-

кущих свойств среды их существования. Такие объекты будут обладать высокоразвитым искусственным интеллектом и демонстрировать роевое поведение. Построение моделей распространения подобных объектов для изучения и борьбы с ними представляет большой научный интерес.

Впервые кинетика развития вирусной эпидемии в адресном пространстве компьютерных сетей была проанализирована с помощью принятых в биологии простых феноменологических SI- и SIR-моделей [1–3]. Под SI-моделью распространения вирусов подразумевают, что любой из компьютеров, входящих в атакуемую сеть, может находиться в одном из двух состояний: уязвимом (S) и инфицированном (I). Согласно этой модели, имеется сеть, состоящая из постоянного числа (N) компьютеров, причем $N = S + I$, а на каждом инфицированном узле может существовать только одна копия червя (вируса), которая *случайным образом* с некоторой *постоянной средней скоростью* атак в единицу времени выбирает в доступном адресном пространстве потенциальную жертву. В модели SIR сетевые узлы существуют в трех состояниях: уязвимом (S), зараженном (I) и невосприимчивом (R). Отметим, что узлы оказываются неуязвимыми только после излечения от инфекции, а N – общее число узлов сети равно $S + I + R$. Вводя *постоянную среднюю скорость иммунизации и атак* в единицу времени для описания динамики развития эпидемий, получают системы дифференциальных кинетических уравнений [1–3], описывающих процесс распространения эпидемии вирусов.

Среди ранних работ стоит упомянуть также статью V. Misra и его коллег [4], которые для моделирования распространения вирусов применили гидродинамическую модель, описывающую указанный процесс как протекание жидкости.

Дальнейшее развитие ранее существовавшие кинетические SI- и SIR-модели получили в работах [5–7]. К примеру, в [5] рассмотрены два типа процессов в компьютерной сети: один – определяемый серверными инфицированными узлами сети, имеющими высокий темп интенсивности вредоносных атак, а другой – инфицированными узлами клиента, имеющими низкий темп интенсивности вредоносных атак. Инфекционные узлы сервера передают вирусы узлам клиента в компьютерной сети, которые, однако, могут излечиваться с течением времени, но при этом снова становятся восприимчивыми к заражению (правда, с меньшей вероятностью). По мнению авторов, это должно создавать эффективную неприкосновенность узлов после некоторого промежутка времени и обеспечивать автоматический защитный механизм от быстро размножающихся вирусов.

Для построения системы кинетических уравнений было выдвинуто предположение, что общее количество компьютерных узлов (N) можно разделить на две группы: N_H, которые имеют высокий темп интенсивности нападения (серверы), и N_L, которые имеют низкий темп интенсивности нападения (клиенты): $N_H + N_L = N$. Группа N_H, в свою очередь, состоит из трех классов: восприимчивые, но еще не зараженные (S_H), иммунизированные и невосприимчивые (A), заразные (I_H): $S_H + A + I_H = N_H$. Группа N_L состоит из четырех классов: восприимчивые (S_L), иммунизированные и невосприимчивые (E_L), заразные (I_L) и вылеченные (R_L): $S_L + E_L + I_L + RL = N_L$. Затем для перечисленных типов узлов была записана система, состоящая из семи кинетических дифференциальных уравнений первого порядка, описывающая переходы между состояниями узлов и их материальный баланс. Моделирование и анализ динамики заражения и равновесия состояний с помощью полу-

ченной системы уравнений и подбора в них величин соответствующих коэффициентов позволил сделать вывод: чтобы получить сеть, свободную от злонамеренных объектов, необходимо обновлять антивирус в нерегулярные интервалы времени, длительность которых определяется кинетическими свойствами вирусной эпидемии.

Предложена кинетическая модель описания развития вирусных эпидемий на основе решения системы трех дифференциальных уравнений первого порядка для баланса узлов, находящихся в уязвимом (S), зараженном (I) и невосприимчивом (R) состояниях [6]. Авторы работы развивают кинетические модели описания вирусных эпидемий в компьютерных сетях на основе представлений об эпидемиологическом пороге, времени ожидания заражения, факторе репликации (коэффициент размножения), вероятности заражения и иммунизации, времени неприкосновенности узла и т. д. В разработанной модели узел, удаленный из зараженного класса (иммунизированный), временно восстанавливается и получает с некоторой вероятностью неприкосновенность, либо он может с некоторой вероятностью снова заразиться. Численное решение полученной системы дифференциальных уравнений [6] показывает возможность развития вирусных эпидемий, имеющих ярко выраженный периодический характер.

На основе кинетических подходов усовершенствованы математические модели распространения компьютерных вирусов в гетерогенной компьютерной сети, учитывающие ее топологические и архитектурные особенности [7]. Обобщенная структура компьютерной сети рассматривалась на основе модели NSIDR: $N = S(t) + I(t) + D(t) + R(t)$, где: N – общее количество объектов в системе; $S(t)$ – количество уязвимых объектов; $I(t)$ – количество зараженных объектов; $D(t)$ – количество объектов, в которых обнаружен вирус; $R(t)$ – количество вылеченных объектов, обладающих иммунитетом. Учет топологических и архитектурных особенностей сетей осуществлялся путем умножения некоторых членов кинетических дифференциальных уравнений на эмпирические поправочные коэффициенты. В частности, для топологии сети «звезда» член, учитывающий убыль (заражение) уязвимых объектов, умножался на коэффициент, равный 0.6. Анализ – на основе данных развития эпидемий – и сравнительные исследования предлагаемых математических моделей позволили сделать вывод о повышении их точности по сравнению с известными математическими моделями и возможности применения разработанных моделей для моделирования вирусных эпидемий в компьютерных сетях [7].

Общие вопросы развития эпидемий вирусов в компьютерных сетях рассмотрены в [8, 9]. В частности, указывается на необходимость разработки стратегий защиты, не уязвимых к изменениям в топологии сети и не требующих знания механизмов развития эпидемии [8]. Например, создание механизмов регулирования числа соединений между узлами в единицу времени и их ограничение при возникновении атак или разработка методов превентивной вакцинации. Обсуждается необходимость разработки контрмер, препятствующих распространению вирусов [9]. Высказывается мнение [9], что выпуск обновлений для программного обеспечения после обнаружения уязвимостей не дает надежной гарантии безопасности. Для повышения уровня защиты авторы [9] предлагают идею выделения в компьютерной сети подсети, в которой будет целенаправленно распространяться антивирус, и поведение этого антивируса будет близко к поведению вредоносного программного обеспечения. Задачей его станет борьба с вирусами, а не

нанесение вреда («хороший вирус» с конкурирующей стратегией распространения). Распространение вирусов и антивирусов будет представлять два конкурирующих процесса, причем для распространения антивирусов возможна реализация двух механизмов: случайная иммунизация и целенаправленная конкурирующая стратегия. Моделирование показало [9], что целенаправленная конкурирующая стратегия борьбы с вирусами наиболее эффективно работает, если скорость распространения антивирусов превышает скорость заражения, а инфицированные узлы могут быть легко идентифицированы. Преимуществом целенаправленной конкурирующей стратегии является отсутствие зависимости ее эффективности от топологии распространения вирусов в компьютерной сети. На основе получаемого результата антивирусные компании смогут использовать социальную сеть своих клиентов или создать сеть из их компьютеров для распространения контрмеры (когда узлы сами могут распространять контрмеры).

Выполнен анализ четырех моделей распространения вирусов [10]: классическая SI-модель, независимая каскадная модель, динамическая модель распространения и модель, учитывающая топологию сетей. Сравнение результатов моделирования показало, что наиболее перспективными с точки зрения разработки механизмов защиты являются модели, основанные на графе сети.

В публикациях последних лет обсуждается разработка интеллектуальных моделей развития и описания вирусных эпидемий в компьютерных сетях, например, подходы, сходные с теорией клеточных автоматов. Так, в [11] рассматривается модель развития вирусной эпидемии не с произвольным порядком распространения вирусов, а с учетом погрешности результатов атак вследствие воздействия вирусов на уже зараженные узлы в сети. С этой целью авторы представляют сеть в виде направленного вероятностного графа (без петель), узлы которого описываются переменными, задающими вероятности их состояния (зараженный, иммунизированный, восприимчивый), а дуги задают взаимодействие между переменными модели. Вирусное распространение определяется характеристиками сети и аналогично действию клеточного автомата. Вирусы могут блуждать в произвольном порядке по пространству графа, иметь различные позиции и скорость. Их перемещение по узлам описывается набором правил. Восприимчивый узел заражается, когда на него попадает вирус; узел, который является носителем болезни, не может быть заражен второй болезнью (т. е. активная болезнь блокирует вторичную инфекцию); иммунизированный узел не может быть заражен повторно и т. д. Следует отметить, что предлагаемый авторами подход устраняет многие проблемы, существовавшие в более ранних эпидемиологических моделях.

Кроме того, очень активно развиваются модели на основе цепей Маркова. В частности, предлагается модель описания развития вирусных эпидемий на основе стохастических моделей интерактивных цепей Маркова [12], в которых состояние узлов сети на каждом следующем шаге развития эпидемии зависит от его состояния и состояния соседей на предыдущем шаге, а сама сеть представляется в виде ненаправленного графа. Использование цепей Маркова, по мнению авторов [12], позволяет оценить защищенность сетей с различной топологией от компьютерных вирусов и выбирать наиболее безопасные сетевые структуры уже на раннем этапе проектирования.

Анализ и моделирование эпидемий вирусов в компьютерных сетях можно осуществлять с использованием методов сопоставления. Например, в [13] для описания эпидемий

двух червей и трояна: (*wormnetsky.p, wormmytob.mr, trdir.stration.ge*) использованы две различных модели: одна – на основе авторегрессионного анализа, другая – на основе Фурье-анализа. Авторегрессионный и Фурье-анализ дают возможность предсказания увеличения и/или уменьшения тенденций в распространении определенного типа вируса (при помощи накопленного по другим эпидемиям опыта). Результаты анализа показывали приемлемую корреляцию времени распространения вирусов между моделями. Разработанная методика позволяет, как полагают авторы [13], предсказывать и управлять уровнями заражения, заранее обеспечивая превентивные меры, увеличивая тем самым безопасность и надежность.

Важной задачей обеспечения надежности работы компьютерных и телекоммуникационных сетей и защиты информации в процессе ее передачи является изучение вопросов образования групп вычислительных узлов компьютерных сетей, физически связанных между собой каналами связи, но по тем или иным причинам блокированных, т. е. исключенных из работы (например, такое поведение возможно при распространении эпидемий компьютерных вирусов). При определенных условиях такие группы блокированных узлов могут увеличиваться в размерах и образовывать кластеры, что приведет к общей потере работоспособности сети по передаче данных. В силу исторически сложившихся обстоятельств любая вычислительная сеть, начиная с уровня района города, имеет нерегулярную случайную структуру. Наиболее ярким примером такой сети является Интернет. Эта нерегулярность определяется множеством факторов, среди которых следует выделить: наличие провайдеров с различным сетевым и коммуникационным оборудованием, переменное число абонентов, постоянно изменяющаяся топология подключения и т. п.

При описании топологии блокирования узлов сетей в случае распространения вирусов в настоящее время преобладает подход, согласно которому развитие эпидемии представляется в виде процесса, напоминающего по своей структуре дерево Кэйли со случайным числом связей [14]. Особое внимание можно обратить на работу [15], в которой описана задача определения вероятности заражения узлов в зависимости от удаленности узла от источника инфекции в сетях с различным масштабом и числом узлов. Топологическими параметрами здесь являлись масштаб и число узлов, однако разнообразие структур сетей в данных работах не исследовалось.

Рассматриваемая в [15] модель использует понятие *scale free graph*, который может иметь любое число узлов. Внешний вид такого графа с общим числом узлов 100 представлен на рис. 1а. Однако на определенном этапе зараженные узлы сети могут отправлять копии вирусов уже на инфицированные, и топология процесса будет иметь вид, представленный на рис. 1б и 1в.

С помощью модели *scale free graph* можно также рассмотреть динамику трафика передачи данных [16, 17], а также процессы иерархического роста сетевой структуры [18].

Очевидно, что если блокированных узлов будет не очень много, то между двумя произвольно выбранными не близлежащими узлами сохранится хотя бы один «открытый» путь (путь, состоящий из неблокированных узлов). Доля блокированных узлов, при которой сеть в целом потеряет работоспособность, назовем порогом перколяции, ниже его значения сеть является работоспособной, несмотря на то, что в ней есть некоторые узлы или их группы (кластеры), блокированные вирусами. Выше порога перколяции вся сеть

целиком выключается и теряет работоспособность по передаче данных. Между двумя произвольно выбранными узлами нет ни одного «открытого» пути.

С целью улучшения технико-экономических и эксплуатационных характеристик сетей и создания новых методов и методологий защиты компьютерных сетей и приложений большой научный и практический интерес для разработки топологии вычислительной сети, имеющей высокую отказоустойчивость, представляет исследование процессов образования кластеров блокированных узлов и перколяции данных в сетях, имеющих различную (в том числе, и случайную) топологию [19, 20].

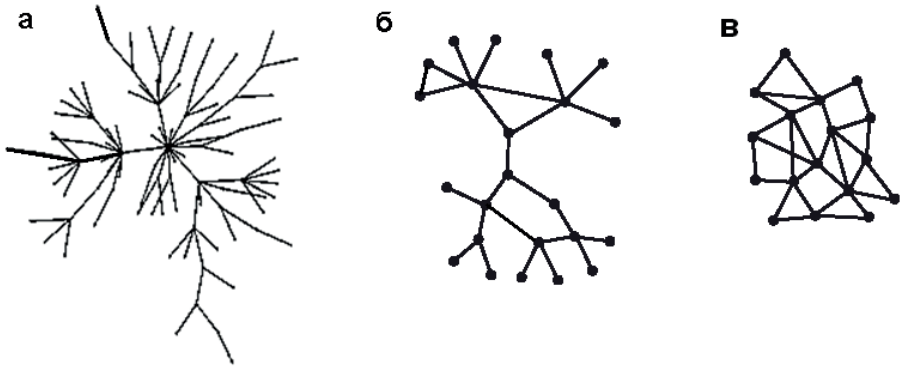

Рис. 1. Общий вид *scale free graph* (а); вид графа зараженных узлов на более поздних этапах вирусной эпидемии (б) – начало процесса взаимных DDoS-атак; процесс взаимных DDoS-атак становится весьма существенным (в).

Для уточнения параметров моделей стоит обсудить два понятия:

- распространение по физическим каналам связи между узлами: два узла являются «соседями», если имеют прямой (без промежуточных посредников) канал связи;
- распространение по адресной связи между узлами: вирус может отправить свою копию не на физического «соседа», а на произвольно выбранный узел со случайным сетевым (IP) адресом.

Во втором случае топология развития вирусной эпидемии имеет вид дерева (сети) Кэйли со случайным числом связей, а в первом – структура физически связанных зараженных узлов будет иметь более сложный вид. Для установления взаимосвязи между процессами, происходящими в адресном и физическом пространствах сети, можно воспользоваться методами теории перколяции. Не исключено, что заражение узла вирусом приведет к его блокировке относительно обработки и передачи данных в компьютерной сети. Важно также отметить, что после 2001 г., когда произошли массовые эпидемии таких червей, как *CodeRed I, CodeRed II, Nimda, Slammer* и ряда других вирусов, выяснилось, что созданные к текущему моменту модели не всегда адекватно описывают процессы распространения вирусов по сети.

Перколяционные свойства сетевых структур

В теории перколяции изучают решения задачи узлов и задачи связей для сетей с различными регулярными (2D-структурами – треугольной, шестиугольной решетками, деревья Кейли и т. д. и 3D-структурами – гексагональной, кубической решетками и т. д.), а также нерегулярными, случайными структурами. Для решения задачи свя-

зей необходимо определить долю связей, которую нужно разорвать, чтобы сеть распалась минимум на две несвязанные части. В задаче узлов необходимо определить долю блокированных узлов, при которой сеть распадется на несвязанные между собой кластеры, внутри которых сохраняются связи. Другой вариант решения – это возможность определить долю проводящих узлов, когда возникает проводимость. Доля неблокированных узлов (в задаче узлов) или неразорванных связей (в задаче связей), при которой возникает проводимость между двумя произвольно выбранными узлами сети, называется порогом перколяции (протекания). Суть перколяционного процесса состоит в изменении общего состояния структуры (сеть работоспособна) на противоположное состояние (сеть не работоспособна) при изменении отдельных свойств элементов (узлов сети).

Понятие долей блокированных узлов или связей является эквивалентным понятию вероятности нахождения случайно выбранного узла (или связи) в блокированном (разорванном) состоянии. Поэтому можно принять, что величина порога перколяции определяет вероятность передачи информации через всю сеть в целом, если блокирована (исключена) некоторая часть ее узлов (или связей), т. е. задана средняя вероятность блокирования узла (разрыва связи). Достижение порога перколяции в сети соответствует кластеру, в котором есть связи между любыми его произвольными узлами (образуется так называемый бесконечный, или стягивающий кластер).

При передаче информации через сеть важным фактором является влияние числа и размера кластеров блокированных (или проводящих) узлов на проводимость сетевой структуры в целом. Применение методов теории перколяции к исследованию сетевых структур и протекающих в них процессов позволяет дать ответы на следующие вопросы [21–23]:

1) нахождение распределения кластеров блокированных узлов сетевой структуры по размерам при заданной вероятности их блокирования;

2) нахождение статистических характеристик кластеров, например, средний размер кластеров блокированных узлов сетевой структуры;

3) как зависит величина порога перколяции сетевой структуры от ее плотности (среднего числа связей, приходящихся на один узел).

Возникают и другие вопросы.

Чтобы построить граф сетевой структуры, рассмотрим следующую модель. Возьмем набор вершин графа (узлы сети – компьютеры, мобильные устройства, сетевое оборудование и т. д.), которые могут быть связаны между собой произвольным образом множественными связями (ребра графа – линии связи). Пример образования такой структуры, полученной путем численного моделирования зависимости порогов перколяции случайных сетей от среднего числа связей в расчете на один узел (плотности) сети, показан на рис. 2 [24, 25]. Решалась и задача блокирования узлов, и задача разрыва связей [23–25]. Проведено численное моделирование зависимости порогов перколяции случайных сетей от среднего числа связей в расчете на один узел (плотности) сети, для структуры, представленной на рис. 2 [23, 24].

Полученные для задачи блокирования узлов результаты для небольших плотностей сетей суммированы в таблице.

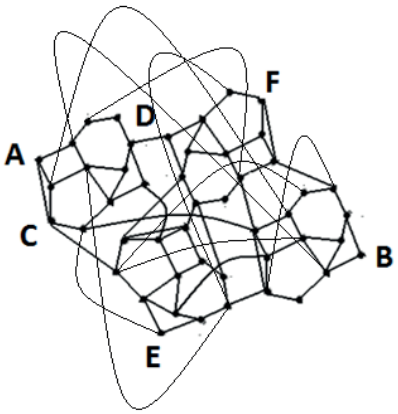

Рис. 2. Структура случайной сети передачи данных [25].

Величина порога перколяции для задачи блокирования узлов случайной сети с множеством путей между узлами [23, 24]

№	Число связей для одного узла сети (плотность). В скобках приведены значения величин обратной плотности	Величина порога перколяции (доля проводящих узлов, при которой возникает проводимость сети в целом). В скобках приведены значения величин натурального логарифма величины порога перколяции
1	2.36 (0.42)	0.52 (-0.65)
2	2.82 (0.35)	0.43 (-0.84)
3	3.29 (0.30)	0.37 (-0.99)
4	4.70 (0.21)	0.27 (-1.31)
5	4.75 (0.21)	0.25 (-1.39)
6	6.17 (0.16)	0.19 (-1.66)
7	6.75 (0.15)	0.18 (-1.71)
8	9.41 (0.11)	0.17 (-1.77)
9	10.02 (0.10)	0.15 (-1.90)

Для случайных структур, величины порогов перколяции которых представлены в таблице, зависимость их натурального логарифма *ln P*(*x*) от обратной величины плотности сети (1/*x*) может быть описана линейным уравнением [24]:

$$\ln P(x) = \frac{4.02}{x} - 2.26 \qquad (1)$$

с величиной коэффициента корреляции числовых данных и уравнения линейной зависимости, равной 0.97.

Полученную зависимость целесообразно использовать для вычисления величин порогов перколяции по величинам плотности сетей. Далее, используя динамическую модель, можно определить время достижения порога и выхода сети (в целом) из работоспособного состояния.

Модель стохастической динамики распространения в компьютерных сетях эволюционирующих вирусов при условии устаревания и запаздывания действия защиты

Теперь обратимся к рассмотрению модели стохастической динамики распространения в компьютерных сетях эволюционирующих вирусов при условии устаревания и

запаздывания действия защиты. Для построения модели стохастической кинетики распространения эволюционирующих (приспосабливающихся или видоизменяющихся под среду) вирусов и кластеризации блокированных узлов компьютерных сетей в адресном пространстве мы разработали и предлагаем следующий подход.

Рассмотрим сеть, в которой происходит процесс распространения вирусов. Он начинается раньше, чем появятся эффективные способы организационного и технического противодействия (антивирусная защита имеет время запаздывания). Долю узлов сети, находящихся в момент времени t в зараженном состоянии, обозначим как $y_1(t)$; в защищенном (иммунизированном) состоянии – $y_2(t)$; в нейтральном состоянии (не инфицирован, не защищен и может быть заражен) обозначим, как $y_3(t)$. Общее число узлов сети примем равным L.

В начальный момент времени ($t = 0$) имеется некоторое количество (или доля $y_1(t = 0)$) зараженных узлов, которые могут рассылать копии вирусов по узлам сети, случайно выбирая их в адресном пространстве. Кроме того, имеется некоторое число узлов сети (или доля $y_2(t = 0)$), которые занимаются борьбой с вирусами (излечивают зараженные и иммунизируют свободные узлы), рассылая копии антивирусов (полезные вирусы) по узлам сети, также случайным образом выбирая их в адресном пространстве, а также $y_3(t = 0)$ – это узлы в нейтральном состоянии (не инфицирован, не защищен и может быть заражен). Антивирусы могут устаревать, вследствие чего ранее иммунизированные узлы могут быть вновь инфицированы. Введем следующие времена: τ_1 – запаздывания действия антивируса, τ_2 – устаревания антивируса (то есть узел становится уязвим для новых видов вирусов спустя некоторое время после иммунизации, что во многом отражает реально существующее положение дел). Необходимо отметить, что если рассматривать модели, в которых рассылка вирусов происходит целенаправленным образом [26] с учетом ранее выбранных узлов в адресном пространстве и интеллектуальных стратегий поведения, то захват сети должен происходить быстрее, так как при случайной рассылке, на завершающем этапе развития эпидемий начинаются взаимные DDoS-атаки инфицированных узлов. Однако в предлагаемой нами модели происходит и процесс иммунизации за счет рассылки антивирусов. Поскольку распространение вирусов и антивирусов является независимым, то, на наш взгляд, для их распространений следует выбирать механизм случайной рассылки.

Описанный нами процесс стохастической кинетики распространения эволюционирующих вирусов в компьютерной сети опишем диаграммой, представленной на рис. 3, и системой кинетических уравнений, приведенной ниже.

$$\frac{dy_1(t)}{dt} = ay_1(t)y_3(t) - by_1(t)y_2(t-\tau_1) \tag{2}$$

$$\frac{dy_2(t)}{dt} = cy_2(t-\tau_1)y_3(t) + by_1(t)y_2(t-\tau_1) - ky_2(t-\tau_2) \tag{3}$$

$$\frac{dy_3(t)}{dt} = -ay_1(t)y_3(t) - cy_2(t-\tau_1)y_3(t) + ky_2(t-\tau_2) \tag{4}$$

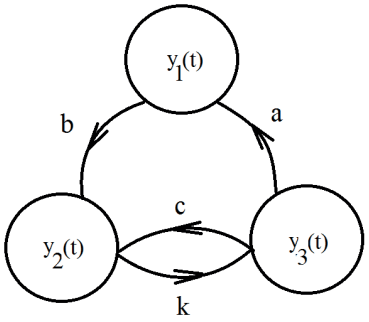

Рис. 3. Диаграмма, описывающая рассматриваемую модель процесса распространения вирусов в компьютерной сети.

Производные по времени определяют скорости изменения долей соответствующих узлов; *a*; *b*; *c* и *k* – некоторые коэффициенты, характеризующие соответствующие переходы на рис. 1 (эти коэффициенты являются интегральными параметрами, зависящими, например, от числа копий рассылаемых вирусов и антивирусов, вероятности встречи и т. д.). Перемножение различных функций (например, $y_1(t)\cdot y_3(t)$) характеризует вероятность соответствующих встреч.

Чтобы пояснить предлагаемую модель, рассмотрим более подробно одно из кинетических уравнений, например, уравнение (3). Член уравнения $\frac{dy_2(t)}{dt}$ описывает скорость изменения доли узлов, находящихся в защищенном (иммунизированном) состоянии, $cy_2(t-\tau_1)y_3(t)$ – определяет прирост за счет иммунизации уязвимых узлов, $by_1(t)y_2(t-\tau_1)$ – определяет прирост за счет излечивания зараженных узлов, $ky_2(t-\tau_2)$ – убыль за счет устаревания антивируса (иммунизированный узел может сначала переходить в незащищенное состояние, а затем заражаться вирусом). Аналогичным образом определяются смысловые значения членов кинетических уравнений (2) и (4).

Достижение порога перколяции сети в модели стохастической динамики распространения в компьютерных сетях эволюционирующих вирусов при условии устаревания и запаздывания действия защиты

Рассмотрим взаимосвязь между долями зараженных, иммунизированных и уязвимых узлов ($y_1(t)$, $y_2(t)$ и $y_3(t)$) при распространении эволюционирующих вирусов в сетях передачи данных и достижении порога перколяции (критической доли зараженных или блокированных узлов). Для обсуждения выберем в качестве примера компьютерную сеть, имеющую случайную структуру, в которой на один узел в среднем может приходиться от 2.5 до 4.0 связей. В соответствии с проведенными по уравнению $ln\ P(x) = 4.02/x - 2.26$ расчетами, общая доля зараженных узлов, при которой сеть потеряет работоспособность, в целом должна составлять от 0.52 (при 2.5 связей на узел порог перколяции равен 0.52) до 0.64 (при 4.0 связей на узел порог перколяции 0.64).

На рис. 4 представлены результаты решения системы уравнений (2)–(4) с взятыми в качестве примера следующими значениями коэффициентов: $a = 0.003$; $b = 0.0015$; $c = 0.0001$ и $k = 0.1$, общим числом узлов сети, равным 1000, временами запаздывания и устаревания $\tau_1 = 38$ и $\tau_2 = 12$ условных единиц, начальными значениями $y_3(t = 0) = 1000$, $y_2(t = 0) = 1$, $y_1(t = 0) = 10$. В данном случае доля зараженных узлов в стационарном состоянии будет достигать 0.64 (кривая 1).

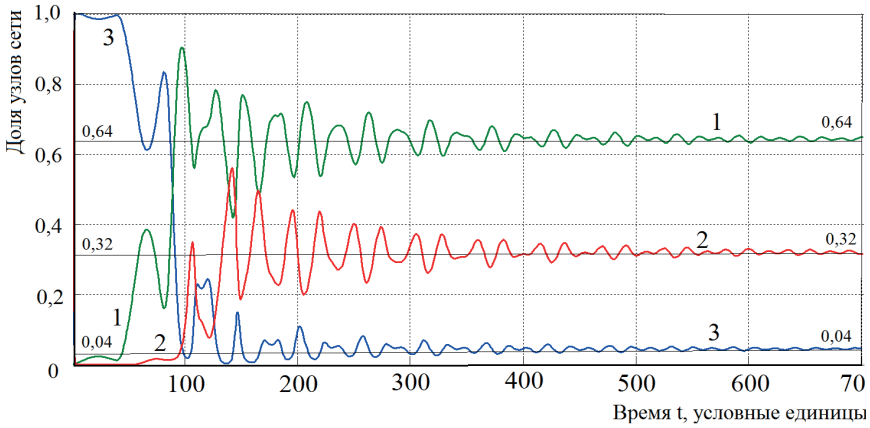

Рис. 4. Кинетика взаимных переходов между узлами компьютерной сети и порог перколяции при распространении эпидемий эволюционирующих вирусов при коэффициентах переходов $a = 0.003$; $b = 0.0015$; $c = 0.0001$; $k = 0.1$.

Сохранение работоспособности сети в целом возможно при условии, чтобы среднее число связей на один ее узел составляло более 4-х (что технологически является нереализуемым в реальной сети с точки зрения стоимостных затрат). Если реализовывать топологии, в которых среднее число связей на один узел будет составлять около 2.5–3.0, то порог перколяции (или возможная доля блокированных узлов) будет иметь величину 0.5. Используя данное значение порога перколяции, можно решить обратную кинетическую задачу и определить необходимые для обеспечения заданного порога перколяции величины коэффициентов: *a, b, c, k* и времена запаздывания и устаревания τ_1 и τ_2. В свою очередь, на основании вычисленных параметров модели может быть задана необходимая надежность, определяемая вероятностями переходов.

Из рис. 4 видно, что доля узлов, находящихся в стационарном защищенном (иммунизированном) состоянии (кривая 2) будет равна 0.32, а доля узлов, находящихся в стационарном нейтральном состоянии (не инфицирован, не защищен и может быть заражен), соответственно, равна 0.04 (кривая 3).

Стохастическая модель блокировки узлов сети и время достижения порога перколяции

Разработанная стохастическая модель блокировки узлов может быть обобщена на уровень сети в целом и связана с результатами, получаемыми в рамках теории перколяции. Для этого нами разработана следующая модель блокировки сети. Предположим, что в некоторый момент времени t доля блокированных (вследствие перегрузок или заражения вирусами) узлов сети передачи данных составляет некоторую величину x_i, которую будем называть состоянием сети. Состояние, наблюдаемое в момент времени t обозначим как x_i ($x_i \in X$). Кроме того, введем интервал времени τ_0, за который возможно изменение состояния x_i. В данном случае любое значение текущего времени $t = h \cdot \tau_0$, где h – номер шага перехода между состояниями (процесс перехода между состояниями становится квазинепрерывным с бесконечно малым временным интервалом τ_0), $h = 0, 1, 2, 3, \ldots, N$. Текущее состояние x_i на шаге h после перехода на шаге $h + 1$ может увеличиваться на некоторую величину ε или уменьшаться на величину ξ и, соответственно, оказаться равным $x_i + \varepsilon$ или $x_i - \xi$. Величины ε и ξ принадлежат области определения x_i и являются па-

раметрами моделируемых процессов. Кроме того, на $x_i + \varepsilon$ и $x_i - \xi$ необходимо наложить ограничения: $x_i + \varepsilon \le K_1$ (K_1 – верхняя граница множества X) и $x - \varepsilon \ge K_2$ (K_2 – нижняя граница множества X). В самом простом случае ε и ξ являются некоторыми постоянными величинами для любого шага *h*.

Введем понятие вероятности нахождения системы в том или ином состоянии. Пусть после некоторого числа шагов *h* про описываемую систему можно сказать, что:

- $P(x - \varepsilon, h)$ – вероятность того, что она находится в состоянии $(x - \varepsilon)$;
- $P(x, h)$ – вероятность того, что она находится в состоянии x;
- $P(x + \xi, h)$ – вероятность того, что она находится в состоянии $(x + \xi)$.

После каждого шага состояние x_i (далее индекс *i* для краткости опускаем) может изменяться на величину ε или ξ. Вероятность $P(x, h + 1)$ того, что на следующем $(h + 1)$-ом шаге система (или процесс) окажется в состоянии x, будет равна (рис. 5):

$$P(x, h + 1) = P(x - \varepsilon, h) + P(x + \xi, h) - P(x, h) \quad (5)$$

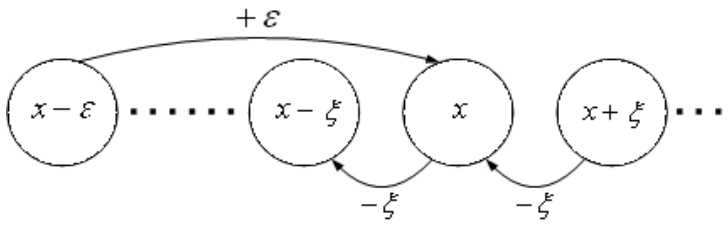

Рис. 5. Схема возможных переходов между состояниями системы (или процесса) на $(h + 1)$-ом шаге.

Поясним уравнение (5) и представленную на рис. 5 схему. Вероятность перехода в состояние x на шаге $h + 1 - P(x, h + 1)$ – определяется суммой вероятностей переходов в это состояние из состояний $(x - \varepsilon) - P(x - \varepsilon, h)$ и $(x + \xi) - P(x + \xi, h)$, в которых находилась система на шаге *h* за вычетом вероятности перехода ($P(x,h)$) системы из состояния x (в котором она находилась на шаге *h*) в любое другое состояние на $(h + 1)$-ом шаге. Будем считать, что сами переходы осуществляются с вероятностью, равной 1.

Учитывая, что $t = h \cdot \tau_0$, где *t* – время процесса, *h* – номер шага, τ_0 – длительность одного шага, можно перейти от *h* к *t*. Разложим уравнение (5) в ряд Тейлора вблизи точки x и, учитывая не более, чем вторые производные, получим (6):

$$\frac{\partial P(x,t)}{\partial t} + \frac{\tau_0}{2}\frac{\partial^2 P(x,t)}{\partial t^2} + \ldots = \frac{\xi - \varepsilon}{\tau_0}\frac{\partial P(x,t)}{\partial x} + \frac{\varepsilon^2 + \xi^2}{2\tau_0}\frac{\partial^2 P(x,t)}{\partial x^2} \quad (6)$$

Член уравнения вида $\frac{\partial P(x,t)}{\partial t}$ определяет общее изменение состояния системы или процесса с течением времени; член уравнения вида $\frac{\partial^2 P(x,t)}{\partial t^2}$ – описывает процесс, при котором состояния сами становятся источниками других состояний (его надо исключить). Член уравнения вида $\frac{\partial P(x,t)}{\partial x}$ – описывает упорядоченный переход либо в состояние, когда оно увеличивается ($\varepsilon > \xi$), либо, когда оно уменьшается ($\varepsilon < \xi$); член уравнения вида $\frac{\partial^2 P(x,t)}{\partial x^2}$ описывает случайное изменение состояния.

Таким образом:

$$\frac{\partial P(x,t)}{\partial t} = a\frac{\partial^2 P(x,t)}{\partial x^2} - b\frac{\partial P(x,t)}{\partial x} \tag{7}$$

где $a = \frac{\varepsilon^{\,2} + \xi^{\,2}}{2\tau_0}$ и $b = \frac{\varepsilon\ - \xi}{\tau_0}$.

Сформулируем и решим для описания работы сети краевую задачу с учетом перколяционных свойств. При числе блокированных узлов в сети $x = \boldsymbol{l}$ работа будет прекращена ($\boldsymbol{l}$ – величина порога перколяции сети). В связи с тем, что мы стремимся избежать этого состояния, необходимо, чтобы выполнялось условие:

$$g(x,\ t)_{x=l} = 0 \tag{8a}$$

Состояние $x = 0$ означает, что в сети нет блокированных узлов. Однако учитывая, что число блокированных узлов не может выходить в область отрицательных значений, мы должны использовать при $x = 0$ условие отражения:

$$g(x,\ t)_{x=0} = 0 \tag{8b}$$

Поскольку в момент времени $t = 0$ в сети уже может быть некоторое число x_0 блокированных узлов, то начальное условие зададим в виде:

$$g(x, t=0) = \delta(x - x_0) = \begin{cases} \int \delta(x - x_0)dx = 1, x = x_0 \\ 0, \neq x_0 \end{cases},$$

Тогда решение уравнения (7), оставаясь непрерывным в точке $x = x_0$, будет испытывать в ней разрыв производной. Решение для $g(x,\ t)$ разбивается на две области при $x > x_0$ и при $x \le x_0$.

Используя методы операционного исчисления для плотности вероятности $g(x,\ t)$ обнаружения состояния системы в одном из значений на отрезке от 0 до l получаем следующую систему уравнений:

При $x > x_0$

$$g_1(x,t) = \frac{2}{l} e^{-\frac{(x_0 - x) + \frac{bt}{2}}{\frac{2a}{b}}} \sum_{n=1}^{M} (-1)^n \sin\left(\pi n \frac{x_0}{l}\right) \sin\left(\pi n \frac{l - x}{l}\right) e^{-\frac{\pi^2 n^2 at}{l^2}} \tag{9}$$

При $x \le x_0$

$$g_2(x,t) = \frac{2}{l} e^{-\frac{(x_0 - x) + \frac{bt}{2}}{\frac{2a}{b}}} \sum_{n=1}^{M} (-1)^n \sin\left(\pi n \frac{x}{l}\right) \sin\left(\pi n \frac{l - x_0}{l}\right) e^{-\frac{\pi^2 n^2 at}{l^2}} \tag{10}$$

И интеграл $P(l,\ t)$:

$$P(l,t) = \int_0^{x_0} g_2(x,t)dx + \int_{x_0}^{l} g_1(x,t)dx \tag{11}$$

будет задавать вероятность того, что состояние системы к моменту времени t находится на отрезке от 0 до l, т. е. ***порог перколяции l*** не будет достигнут, и сеть не окажется блокированной (продолжит выполнять функции передачи данных).

Соответственно, вероятность $Q_t(l, t)$ того, что ***порог перколяции l*** окажется к моменту времени t достигнутым или превзойденным, можно определить следующим образом:

$$Q(l,t) = 1 - P(l,t) \tag{12}$$

Если мы возьмем произвольное значение x_0, ε и ξ (ε > ξ), например $x_0 = 0.05$, ε = 0.015 и ξ = 0.007, то можем построить зависимость достижения порога перколяции от времени. На рис. 6 представлена такая зависимость (от времени вероятности $Q_t(l, t)$ того, что к моменту времени t окажется достигнутым порог перколяции).

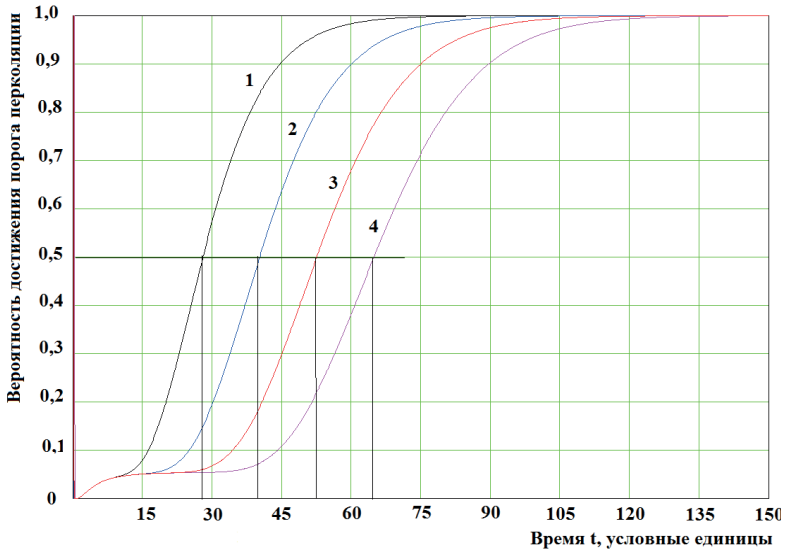

Рис. 6. Зависимость значения вероятности достижения порога перколяции сети от времени. Кривая 1 построена для значения порога перколяции сети $l_1 = 0.30$, кривая 2 – для $l_2 = 0.40$, кривая 3 – для $l_3 = 0.50$ и кривая 4 – для $l_4 = 0.60$.

Полученные результаты можно связать с результатами рассмотрения перколяционной модели. Пересечение горизонтальной линии на рис. 6 с кривыми линиями, описывающими поведение вероятностей, позволяет определить время достижения порога перколяции при заданных параметрах моделирования, а, следовательно, и потерю работоспособности всей сети. Для кривой 1 оно составит порядка 28.0 условных единиц; для кривой 2 – 40.5; кривой 3 – 52.5 и для кривой 4 – 65.0 условных единиц.

Заключение и выводы

1. Для установления взаимосвязи между процессами, происходящими в адресном и физическом пространствах сети целесообразно воспользоваться методами теории перколяции. В сетях передачи данных реализуются различные процессы: блокирование узлов, образование кластеров блокированных узлов, достижение такой количественной доли, при которой вся сеть целиком теряет работоспособность (достижение порога перколяции), несмотря на то, что значительная часть узлов все еще находится в рабочем состоянии. При среднем числе связей на один узел сети передачи данных в диапазоне значе-

ний от 2.5 до 3.5 доля неблокированных узлов, при которой сеть еще сохраняет общую работоспособность, должна иметь значения от 0.52 до 0.37. Используя данные значения порогов перколяции, можно решить обратную кинетическую задачу и определить необходимые для обеспечения заданного порога перколяции величины коэффициентов в стохастической кинетической модели распространения эволюционирующих вирусов. В свою очередь, на основании вычисленных параметров модели может быть задана необходимая надежность оборудования и программного обеспечения работы сетей, определяемая вероятностями переходов в кинетической модели.

2) Рассмотрена новая модель распространения эволюционирующих вирусов: эволюционные свойства вирусов учитываются в модели формальным правилом, согласно которому ранее иммунизированные или вылеченные узлы, через некоторый интервал времени (величина которого является параметром модели), могут быть снова инфицированы, а воздействие антивирусной защиты имеет время запаздывания (которое также является параметром модели). В рамках предлагаемой модели принято, что любой узел сети может находиться в одном из трех состояний: в защищенном (иммунизированном) состоянии, когда он сам рассылает антивирусы (излечивает зараженные и иммунизирует свободные узлы) по узлам сети, случайным образом выбирая их в адресном пространстве (стохастичность поведения); в зараженном состоянии (может рассылать копии вирусов по узлам сети, случайно выбирая их в адресном пространстве, также, стохастичность поведения), и в нейтральном состоянии (может быть заражен).

3) Модель стохастической динамики распространения эволюционирующих вирусов в компьютерной сети описывается в графическом виде с помощью диаграммы возможных переходов между состояниями узлов. Такая запись позволила получить систему кинетических дифференциальных уравнений, описывающих указанные процессы. Анализ полученных решений показывает возможность существования в рамках модели различных режимов распространения вирусов, причем для некоторых наборов величин коэффициентов дифференциальных уравнений наблюдается осциллирующий и почти-периодический характер распространения вирусных эпидемий, что в значительной степени совпадает с реальными наблюдениями.

4) Разработанная на основе кинетических дифференциальных уравнений модель может быть модифицирована и расширена через создание более сложных графических диаграмм изменения состояний и переходов между ними. В частности, это позволяет дополнить систему кинетических уравнений членом, учитывающим общий рост числа пользователей и устройств в компьютерных сетях с течением времени (такой рост, в принципе, описывается функцией любого вида).

5) При описании процесса распространения вирусных эпидемий в вычислительных сетях можно рассматривать совокупность случайных переходов между состояниями всей сети в целом (изменение числа блокированных и разблокированных узлов). Такая формализация позволяет вывести дифференциальное уравнение второго порядка (типа уравнения Колмогорова), описывающее стохастическую динамику изменения состояний как отдельных узлов, так сети в целом. Полученные уравнения для описания динамики стохастического изменения состояний узлов и сети в целом позволяют сформулировать и решить краевые задачи изменения загруженности и блокировки сети, во взаимосвязи

с результатами, получаемыми из перколяционных моделей (например, определить время потери работоспособности сети).

6) Практические рекомендации для защиты любых сетей от угроз вирусных атак заключаются в том, что в случае использования однотипного оборудования и программного обеспечения для создания сетей передачи данных, имеющих среднее число связей в расчете на один узел сети от 2.5 до 3.5, доля такого оборудования должна находиться в пределе от 0.48 (если блокируется 48% используемого оборудования, то все еще выполняется условие перколяции, так как доля не блокированных узлов равна 0.52) до 0.63 (превышать 48–63%). При этом нижняя граница отвечает за эффективное использование ресурсов, а верхняя – за предельно допустимые риски.

Литература:

1. Anderson H., Britton T. Stochastic Epidemic Models and Their Statistical Analysis. NY: Springer-Verlag New-York, Inc., 2000. 133 p.

2. Earn David J.D., Rohani Pejman, Bolker Benjamin M., Grenfell Bryan T. A simple model for complex dynamical transitions in epidemics // Science. 2000. V. 287. P. 667–670. DOI: 10.1126/science.287.5453.667

3. Wang C., Knight J. C., Elder M. C. Impact of network structure on malware propagation: A growth curve perspective // J. Manag. Inform. Syst. 2016. V. 33. № 1. P. 296–325. DOI: 10.1080/07421222.2016.1172440

4. Misra V., Gong W., Towsley D. Fluid-based analysis of a network of AQM routers supporting TCP flows with an application to RED // ACM/SIGCOMM Computer Commun. Rev. 2000. V. 30(4). P. 151–160. DOI: 10.1145/347059.347421

5. Kumar M., Kumar M.B., Panda T.C. A new model on the spread of malicious objects in computer network // Int. J. Hybrid Inform. Technol. 2013. V. 6. № 6. P. 161–176. DOI: 10.14257/ijhit.2013.6.6.14

6. Kumar M.B., Mursalin A.G. Differential epidemic model of virus and worms in computer network // Int. J. Network Security. 2012. V. 14. № 3. P. 149–155.

7. Семенов С.Г., Давыдов В.В. Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом // Вестник Нац. техн. ун-та "ХПИ". 2012. № 38. С. 163–171.

8. Balthrop J., Forrest S., Newman M.E.J., Williamson M.M. Technological networks and the spread of computer viruses // Science. 2004. V. 304. P. 527–529. DOI: 10.1126/science.1095845

9. Chen Li-Chiou, Carley K.M. The impact of countermeasure propagation on the prevalence of computer viruses // IEEE Trans. on Systems, Man, and Cybernetics. Part B: Cybernetics. 2004. V. 34. № 2. P. 823–833.

10. Ojugo A.A., Aghware F.O., Yoro R.E., Yerokun M.O., Eboka A.O., Anujeonye C.N., Efozia F.N. Evolutionary model for virus propagation on networks // Automation, Control and Intelligent Systems. 2015. V. 3(4). P. 56–62. doi: 10.11648/j.acis.20150304.12

11. Vălean H., Pop A., Avram C. Intelligent model for virus spreading // Proceed. of the Int. Symp. on System Theory, Automation, Robotics, Computers, Informatics, Electronics and

Instrumentation. SINTES 13. 18-20 October 2007, Craiova, Romania. P. 117–122.

12. Далингер Я.М., Бабанин Д.В., Бурков С.М. Математические модели распространения вирусов в компьютерных сетях различной структуры // Моделирование систем. 2011. № 4(30). С. 3–11.

13. Piqueira Jos´e R.C., Cesar F.B. Dynamical models for computer viruses propagation // Mathem. Problems in Engineering. Volume 2008. Article ID 940526. 11 pages. doi:10.1155/2008/940526.

14. Nazario J. Defense and Detection Strategies against Internet Worms. Artech House Publ., 2004. 319 p.

15. Pastor-Satorras R., Vespignani A. Epidemics and immunization in scale-free networks / In: Handbook of Graphs and Networks: From the Genome to the Internet / S. Bornholdt and H. G. Schuster (eds.). Wiley-VCH, 2005. DOI: 10.1002/3527602755.ch5.

16. Fekete A., Vattay G., Kocarev L. Traffic dynamics in scale-free networks // Complexus. 2006. V. 3. P. 97–107. DOI: 10.1159/000094192.

17. Wu Zhi-Xi, Peng G., Wong Wing-Ming, Yeung Kai-Hau. Improved routing strategies for data traffic in scale-free networks // J. Statist. Mechanics: Theory and Experiment. 2008. P11002. DOI:10.1088/1742-5468/2008/11/P11002.

18. Boccaletti S., Hwang D.-U., Latora V. Growing hierarchical scale-free networks by means of nonhierarchical processes // Int. J. Bifurcation and Chaos. 2007. V. 17. № 7. P. 2447–2452. DOI:10.1142/S0218127407018518.

19. Zhukov D., Lesko S., Lobanov D. Modeling of open network reliability including the Internet based on the theory of percolation in two-dimensional and three-dimensional regular and random network structures // Proceed. of the Int. Conf. “Internet Computing and Big Data” (ICOMP'14) - WORLDCOMP'14; 2014. V. 3. P. 132–136.

20. Zhukov D., Lesko S. The percolation theory based analysis of data transmission reliability via data communication networks with random structure and kinetics of nodes blocking by viruses // ICNS 2015: Proceed. of the Eleventh Int. Conf. on Networking and Services. May 24-29, 2015. Rome, Italy. P. 24–30.

21. Sahini M., Sahimi M. Applications of Percolation Theory. CRC Press, 2003. 276 p.

22. Stauffer D., Aharony A. Introduction to Percolation Theory. London: Tailor & Francis, 2003. 192 p.

23. Тарасевич Ю.Ю. Перколяция: теория, приложения, алгоритмы. М.: УРСС, 2002. 112 с.

24. Zhukov D., Khvatova T., Lesko S., Zaltsman A. Managing social networks: applying the Percolation theory methodology to understand individuals’ attitudes and moods // Technol. Forecasting and Social Change. 2018. V. 12. P. 297–307. DOI: 10.1016/j.techfore.2017.09.039

25. Zhukov D.O., Khvatova T.Yu., Lesko S.A., Zaltsman A.D. The influence of the connections density on clusterisation and percolation threshold during information distribution in social networks // Informatics and its Applications. 2018. V. 12. Iss. 2. P. 90–97. DOI: 10.14357/19922264180123

26. Жуков Д.О., Гусаров А.Н., Косырева А.В. Исследование эффективных стратегий распространения компьютерных угроз // Вестник компьют. и информ. технологий. 2010. № 7(73). С. 40–46.

References:

1. Anderson H., Britton T. Stochastic Epidemic Models and Their Statistical Analysis. NY: Springer-Verlag, New-York, Inc., 2000. 133 p.

2. Earn David J.D., Rohani Pejman, Bolker Benjamin M., Grenfell Bryan T. A simple model for complex dynamical transitions in epidemics. *Science.* 2000; 287:667-670. DOI: 10.1126/science.287.5453.667

3. Wang C., Knight J. C., Elder M. C. Impact of network structure on malware propagation: A growth curve perspective. *J. Manag. Inform. Syst.* 2016; 33(1):296-325. DOI: 10.1080/07421222.2016.1172440

4. Misra V., Gong W., Towsley D. A fluid based analysis of a network of AQM routers supporting TCP flows with an application to RED. *ACM/SIGCOMM Computer Commun. Rev.* 2000; 30(4):151-160. DOI: 10.1145/347059.347421

5. Kumar M., Kumar M.B., Panda T.C. A new model on the spread of malicious objects in computer network. *Int. J. Hybrid Inform. Technol.* 2013; 6(6):161-176. DOI: 10.14257/ijhit.2013.6.6.14

6. Kumar M.B., Mursalin A.G. Differential epidemic model of virus and worms in computer network. *Int. J. Network Security.* 2012; 14(3):149-155.

7. Semenov S.G., Davydov V.V. Mathematical model of computer virus distribution in heterogeneous computer networks of automated process control systems. *Vestnik NTU "KhPI"* (Bulletin of the National Technical University "Kharkiv Polytechnic Institute"). 2012; 38:163-171. (in Russ.)

8. Balthrop J., Forrest S., Newman M.E.J., Williamson M.M. Technological networks and the spread of computer viruses. *Science.* 2004; 304:527-529. DOI: 10.1126/science.1095845

9. Chen Li-Chiou, Carley K.M. The impact of countermeasure propagation on the prevalence of computer viruses. *IEEE Trans. on Systems, Man, and Cybernetics. Part B: Cybernetics.* 2004; 34(2):823-833.

10. Ojugo A.A., Aghware F.O., Yoro R.E., Yerokun M.O., Eboka A.O., Anujeonye C.N., Efozia F.N. Evolutionary model for virus propagation on networks. *Automation, Control and Intelligent Systems.* 2015; 3(4):56-62. doi: 10.11648/j.acis.20150304.12

11. Vălean H., Pop A., Avram C. Intelligent model for virus spreading. Proceed. of the Int. Symp. on System Theory, Automation, Robotics, Computers, Informatics, Electronics and Instrumentation. SINTES 13. 18-20 October 2007, Craiova, Romania. P. 117-122.

12. Dalinger Ya.M., Babanin D.V., Burkov S.M. The mathematical models of the spreading of viruses in computer networks with the different structures. *Informatika i sistemy upravleniya* (Information Science and Control Systems). 2011; 4(30):3-11. (in Russ.)

13. Piqueira Jos´e R.C., Cesar F.B. Dynamical models for computer viruses propagation. *Mathem. Problems in Engineering.* Volume 2008; Article ID 940526: 11 pages. doi:10.1155/2008/940526.

14. Nazario J. Defense and Detection Strategies against Internet Worms. Artech House Publ., 2004. 319 p.

15. Pastor-Satorras R., Vespignani A. Epidemics and immunization in scale-free networks. In: Handbook of Graphs and Networks: From the Genome to the Internet. S. Bornholdt and H. G. Schuster (eds.). Wiley-VCH, 2005. DOI: 10.1002/3527602755.ch5.

16. Fekete A., Vattay G., Kocarev L. Traffic dynamics in scale-free networks. *Complexus*. 2006; 3: 97-107. DOI: 10.1159/000094192.

17. Wu Zhi-Xi, Peng G., Wong Wing-Ming, Yeung Kai-Hau. Improved routing strategies for data traffic in scale-free networks. *J. Statist. Mechanics: Theory and Experiment.* 2008; P11002. DOI:10.1088/1742-5468/2008/11/P11002.

18. Boccaletti S., Hwang D.-U., Latora V. Growing hierarchical scale-free networks by means of nonhierarchical processes. *Int. J. Bifurcation and Chaos.* 2007; 17(7):2447-2452. DOI:10.1142/S0218127407018518.

19. Zhukov D., Lesko S., Lobanov D. Modeling of open network reliability including the Internet based on the theory of percolation in two-dimensional and three-dimensional regular and random network structures. Proceed. of the Int. Conf. "Internet Computing and Big Data" (ICOMP'14) - WORLDCOMP'14; 2014; 3:132-136.

20. Zhukov D., Lesko S. The percolation theory based analysis of data transmission reliability via data communication networks with random structure and kinetics of nodes blocking by viruses. ICNS 2015: Proceed. of the Eleventh Int. Conf. on Networking and Services. May 24-29, 2015. Rome, Italy. P. 24-30.

21. Sahini M., Sahimi M. Applications of Percolation Theory. CRC Press, 2003. 276 p.

22. Stauffer D., Aharony A. Introduction to Percolation Theory. London: Tailor & Francis, 2003. 192 p.

23. Tarasevich Yu.Yu. Percolation: theory, applications, algorithms. M.: Editorial URSS, 2002. 112 p. (in Russ.)

24. Zhukov D., Khvatova T., Lesko S., Zaltsman A. Managing social networks: applying the Percolation theory methodology to understand individuals' attitudes and moods. *Technol. Forecasting and Social Change.* 2018; 129:297-307. DOI: 10.1016/j.techfore.2017.09.039

25. Zhukov D.O., Khvatova T.Yu., Lesko S.A., Zaltsman A.D. The influence of the connections density on clusterisation and percolation threshold during information distribution in social networks. *Informatics and its Applications.* 2018; 12(2):90-97. DOI: 10.14357/19922264180123

26. Zhukov D.O., Gusarov A.N., Kosyreva A.V. Computer threats distribution effective strategy research. *Vestnik komp'yuternykh i informasionnykh tekhnologij* (Herald of Computer and Information Technologies). 2010; 7 (73):40-46. (in Russ.)

Об авторах:

Лесько Сергей Александрович, кандидат технических наук, доцент кафедры «Управление и моделирование систем» Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Алёшкин Антон Сергеевич, кандидат технических наук, доцент кафедры «Информационное противоборство» Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Филатов Вячеслав Валерьевич, кандидат технических наук, заместитель заведующего кафедрой «Управление и моделирование систем» Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

About the authors:

Sergey A. Lesko, Ph.D. (Engineering), Associate Professor of the Chair "Management and Modeling of Systems", Institute of Integrated Security and Special Instrumentation, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Anton A. Alyoshkin, Ph.D. (Engineering), Associate Professor of the Chair "Information Confrontation", Institute of Integrated Security and Special Instrumentation, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Vyacheslav V. Filatov, Ph.D. (Engineering), Deputy Head of the Chair "Management and Modeling of Systems", Institute of Integrated Security and Special Instrumentation, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Для цитирования: Лесько С.А., Алёшкин А.С., Филатов В.В. Стохастические и перколяционные модели динамики блокировки вычислительных сетей при распространении эпидемий эволюционирующих компьютерных вирусов // Российский технологический журнал. 2019. Т. 7. № 3. С. 7–27. DOI: 10.32362/2500-316X-2019-7-3-7-27

For citation: Lesko S.A., Alyoshkin A.S., Filatov V.V. Stochastic and percolating models of blocking computer networks dynamics during distribution of epidemics of evolutionary computer viruses. *Rossiyskiy tekhnologicheskiy zhurnal* (Russian Technological Journal). 2019; 7(3):7-27. (in Russ.). DOI: 10.32362/2500-316X-2019-7-3-7-27