ВЕСТНИК ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
2020 Управление, вычислительная техника и информатика № 52

УДК 519.872
DOI: 10.17223/19988605/52/3

С.А. Лесько, Д.О. Жуков, Л.А. Истратов

МОДЕЛИ ОПИСАНИЯ ДИНАМИКИ БЛОКИРОВКИ УЗЛОВ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ ВИРУСАМИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ПЕРКОЛЯЦИОННЫХ, КИНЕТИЧЕСКИХ И СТОХАСТИЧЕСКИХ МЕТОДОВ

Представлен комплекс моделей динамики блокирования узлов вычислительных сетей, созданных на основе учета их перколяционных свойств и механизмов изменения состояний (кинетического и стохастического). В кинетической модели процессы распространения эволюционирующих вирусов и достижение порога перколяции рассматриваются на основе систем дифференциальных уравнений, а в модели стохастической динамики – на основе рассмотрения схем вероятностей переходов между состояниями сети и решения краевой задачи.
Ключевые слова: блокирование узлов сети; порог перколяции сети; кинетическая модель блокирования узлов; стохастическая динамика блокирования узлов.

Впервые кинетика развития вирусной эпидемии в адресном пространстве компьютерных сетей и блокировка их узлов были проанализированы с помощью принятых в биологии простых феноменологических SI и SIR моделей [1–3]. Под моделью SI 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, которая *случайным образом* выбирает в доступном адресном пространстве потенциальную жертву с некоторой *постоянной средней скоростью* атак в единицу времени.

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 можно получить системы дифференциальных кинетических уравнений [Ibid.], описывающих процесс распространения эпидемии вирусов. Кроме того, среди ранних публикаций можно упомянуть оригинальную работу [4], в которой для моделирования распространения вирусов применили гидродинамическую модель, и этот процесс рассматривался как протекание жидкости.

Дальнейшее развитие кинетические модели SI и SIR получили в работах [5–7]. В [5] было рассмотрено два типа процессов в компьютерной сети: один определяется 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 становится восприимчивыми к заражению, но с меньшей вероятностью. В работе [6] рассматривается кинетическая модель 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 работе [7] были усовершенствованы математические модели распространения компьютерных вирусов в гетерогенной компьютерной сети, учитывающие ее топологические и архитектурные особенности. Обобщенная структура компьютерной сети рассматривалась на основе модели PSIDR: $N = S(t) + I(t) + D(t) + R(t)$, где N – общее количество объектов

в системе, $S(t)$ – количество уязвимых объектов, $I(t)$ – количество зараженных объектов, $R(t)$ – количество вылеченных объектов, обладающих иммунитетом, $D(t)$ –количество объектов, в которых обнаружен вирус. Учет топологических и архитектурных особенностей сетей осуществлялся за счет 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.

Общие вопросы развития эпидемий вирусов в компьютерных сетях были рассмотрены в работах [8, 9]. В частности, в [8] указывается на необходимость разработки стратегий защиты, неуязвимых к изменениям в топологии сети и не требующих знания механизмов развития эпидемии. Например, создание механизмов регулирования числа соединений между узлами в единицу времени и их ограничение при возникновении атак или разработка методов превентивной вакцинации. В статье [9] обсуждаются вопросы разработки контрмер, препятствующих распространению вирусов. Авторы работы утверждают, что выпуск обновлений для программного обеспечения после обнаружения уязвимостей не дает надежной гарантии по безопасности. Для повышения уровня защиты они предлагают идею, согласно которой в компьютерной сети необходимо выделить подсеть, где будет целенаправленно распространяться антивирус, задачей которого станет борьба с вирусами.

В работе [10] проводится анализ четырех моделей распространения вирусов: классическая модель SI, 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 описании графа сети.

В работе [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 сети. Для этого 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 графической модели. Вирусное распространение определяется характеристиками сети и похоже на действие клеточного автомата.

В публикации [12] рассматривается модель описания развития вирусных эпидемий на основе стохастических моделей интерактивных цепей Маркова, 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.

Для анализа и моделирования эпидемий вирусов в компьютерных сетях можно использовать методы сопоставления. В работе [13] описано две модели: одна на основе авторегрессионного анализа, а другая на основе Фурье-анализа. Результаты анализа показывают приемлемую корреляцию между временем распространением вирусов. Авторегрессионный и Фурье-анализ представляют возможность предсказания усиления и ослабления тенденций в распространении определенного типа вируса при помощи накопленного опыта по другим эпидемиям.

При описании топологии блокирования узлов сетей при распространении 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]. Можно обратить внимание на работу [15], в которой рассматривается 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.

Очевидно, что если блокированных узлов будет не очень много, то между двумя произвольно выбранными неблизлежащими узлами будет сохраняться хотя бы один «отрытый» путь (путь, состоящий из неблокированных узлов). Доля блокированных узлов, при которой сеть в целом потеряет работоспособность, будем называть 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.

Следует отметить, что имеется много работ, в которых описаны исследования перколяционных свойств сетевых структур [16–22]. Однако никто не изучал взаимосвязи структурных свойств сетей и динамики их блокирования.

Исследование процессов образования кластеров блокированных узлов и перколяции данных в сетях, имеющих различную (в том числе и случайную) топологию, представляет большой научный и практический интерес для разработки топологии вычислительных сетей, имеющих высокую отказоустойчивость, и создания новых методов и методологии защиты компьютерных сетей.

1. Перколяционные свойства сетевых структур

В теории перколяции (теория вероятностей на графах) изучают решение задачи узлов и задачи связей для сетей с различной – как регулярной (2D-структуры – треугольная, шестиугольная, деревья Кейли и т.д.; 3D – гексагональная, кубическая и т.д.), так и случайной – структурой. При решении задачи связей определяют долю связей, которую нужно разорвать, чтобы сеть распалась минимум на две несвязанные части. В задаче узлов определяют долю блокированных узлов, при которой сеть распадется на несвязанные между собой кластеры, внутри которых сохраняются связи (или, наоборот, долю проводящих узлов, когда проводимость возникает). Доля блокированных узлов (в задаче узлов) или разорванных связей (в задаче связей), при которой исчезает проводимость между двумя произвольно выбранными узлами сети, называется порогом перколяции (протекания).

Определение долей блокированных узлов или связей эквивалентно нахождению вероятности случайно выбранного узла (или связи) быть в блокированном (разорванном) состоянии. Поэтому 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).

В работах [23, 24] было проведено численное моделирование зависимости порогов перколяции случайных сетей от среднего числа связей в расчете на один узел (плотность) сети. Полученные в этих работах результаты для задачи блокирования узлов при небольших плотностях сетей показывают, что для случайных структур зависимость их натурального логарифма $\ln P(x)$ от обратной величины плотности сети ($1/x$) может быть описана уравнением

$$\ln P(x) = \frac{4,02}{x} - 2,26 \qquad (1)$$

с величиной коэффициента корреляции числовых данных и уравнения линейной зависимости, равным 0,97.

Данная зависимость может быть использована для вычисления по величинам плотности сетей их порогов перколяции. Далее, используя динамические модели, можно определить время достижения и выхода сети из работоспособного состояния в целом.

Рассмотрим две разработанные нами модели блокировки узлов сетей с течением времени и достижения величины порога блокирования (перколяции).

2. Кинетика распространения в компьютерных сетях эволюционирующих вирусов при условии устаревания и запаздывания действия защиты и достижение порога перколяции

Рассмотрим сеть, в которой происходит процесс распространения вирусов, начинающийся 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) – $y_3(t)$. Общее число узлов сети примем равным L. В начальный момент времени ($t = 0$) имеется некоторое количество ($y_1(t = 0)$) зараженных узлов, которые могут рассылать копии вирусов по узлам сети, случайно выбирая их в адресном пространстве. Кроме того, имеется некоторое число узлов сети ($y_2(t = 0)$), которые занимаются борьбой с вирусами (излечивают зараженные и иммунизируют свободные узлы), рассылая копии антивирусов (полезные вирусы) по узлам сети, случайным образом выбирая их в адресном пространстве, и $y_3(t = 0)$ – 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, т.е. узел становится уязвимым для новых видов вирусов спустя некоторое время после иммунизации. Поскольку распространение вирусов и антивирусов является независимым, то для их распространения следует выбрать механизм случайной рассылки.

Описанный процесс стохастической кинетики распространения эволюционирующих вирусов в компьютерной сети можно описать диаграммой, представленной на рис. 1, и системой кинетических уравнений

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

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

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

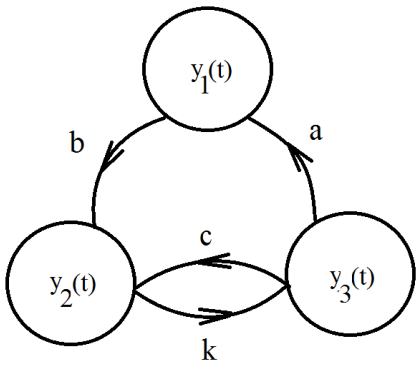

Рис. 1. Диаграмма, описывающая рассматриваемую модель процесса распространения вирусов в компьютерной сети
Fig. 1. Diagram describing the considered model of the process of spreading viruses in a computer network

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 $y_1(t)y_3(t)$, характеризует вероятность соответствующих встреч.

Для пояснения модели рассмотрим более подробно одно из кинетических уравнений, например (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, $by_1(t)y_2(t-\tau_1)$ –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 определяется смысловое значение членов кинетических уравнений (2) и (4).

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 достижением 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 (1) 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. 2 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 1 000, временами запаздывания и устаревания τ_1 = 38 и τ_2 = 12 условных единиц, начальными значениями $y_3(t = 0)$ = 1 000, $y_2(t = 0)$ = 1, $y_1(t = 0)$ =10. В данном случае доля зараженных узлов в стационарном состоянии будет достигать 0,64 (см. рис. 2, кривая *1*). Для того чтобы сеть в целом оставалась работоспособной, необходимо, чтобы среднее число связей на один ее узел составляло более 4, 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 времен запаздывания и устаревания τ_1 и τ_2. В свою очередь, на основании вычисленных параметров модели может быть задана необходимая надежность, определяемая вероятностями переходов.

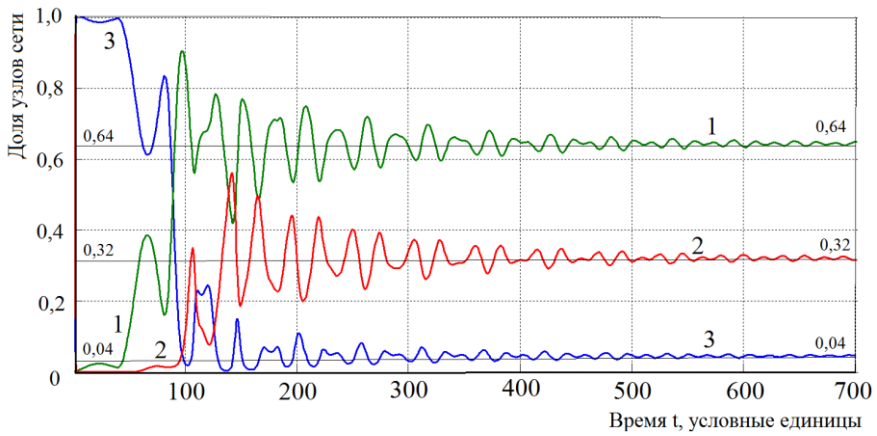

Рис. 2. Кинетика взаимных переходов между узлами компьютерной сети и порог перколяции при распространении эпидемий эволюционирующих вирусов при коэффициентах переходов: a = 0,003; b = 0,0015; c = 0,0001; k = 0,1

Fig. 2. Kinetics of mutual transitions between computer network nodes and the percolation threshold for the spread of epidemics of evolving viruses with transition coefficients: a = 0,003; b = 0,0015; c = 0,0001; k = 0,1

Доля узлов, находящихся при стационарном состоянии в защищенном (иммунизированном) состоянии (см. рис. 2, кривая *2*) будет равна 0,32, доля узлов, находящихся при стационарном состоянии в нейтральном состоянии (не инфицирован, не защищен и может быть заражен) – 0,04 (см. рис. 2, кривая *3*).

3. Стохастическая модель блокировки узлов сети и время достижения порога перколяции

Предположим, что в некоторый момент времени t доля блокированных (вследствии перегрузок или заражения вирусами) узлов сети передачи данных составляет некоторую величину x_i, которую будем называть состоянием сети.

Состояние, наблюдаемое в момент времени *t*, можно обозначить, 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 $t = h\tau_0$, 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 шаг $h + 1$ 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 xi и являются параметрами 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 $x_i - \xi \ge K_2$ (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 состояния. 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 можно опустить) может изменяться на величину ε или ξ.

Вероятность $P(x, h + 1)$ того, что на следующем, $(h + 1)$-м, шаге система (или процесс) окажется в состоянии x, будет равна (см. рис. 3)

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

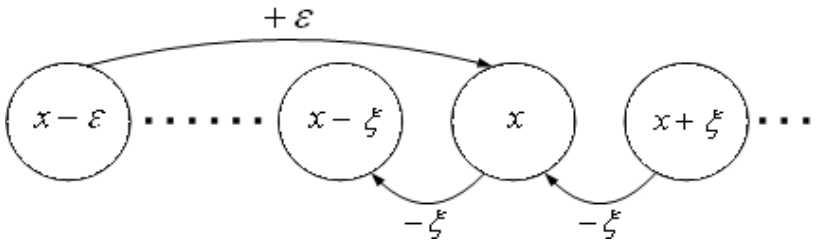

Рис. 3. Схема возможных переходов между состояниями системы (или процесса) на $(h + 1)$-м шаге
Fig. 3. Diagram of possible transitions between system states (or process) at $h + 1$ step

Поясним уравнение (5) и представленную на рис. 3 схему. Вероятность перехода в состояние x на шаге h $P(x, h + 1)$ 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 $(h + 1)$-м шаге. Будем считать, что сами переходы осуществляются с вероятностью, равной 1.

Учитывая, что $t = h\tau_0$, где t – время процесса, h – номер шага, τ_0 – длительность одного шага, перейдем от h к t. Разложим уравнение (5) в ряд Тейлора в близи точки x. Далее, перейдя от вероятности к плотности вероятности ($\rho(x,t) = \dfrac{dP(x,t)}{dx}$) и учитывая не более чем вторые производные, получим:

$$\frac{d\rho(x,t)}{dt} = a\frac{d^2\rho(x,t)}{dx^2} - b\frac{d\rho(x,t)}{dx}, \quad (6)$$

где $a = \dfrac{\varepsilon^2 + \xi^2}{2\tau}$, $b = \dfrac{\varepsilon - \xi}{\tau}$.

Член уравнения вида $\dfrac{d\rho(x,t)}{dt}$ определяет общее изменение состояния системы или процесса с течением времени. Член уравнения вида $\dfrac{d^2\rho(x,t)}{dt^2}$ описывает процесс, при котором состояния сами

становятся источниками других состояний (поэтому он был исключен). Отметим также, что член уравнения $\frac{d\rho(x,t)}{dt}$ описывает упорядоченный переход либо в состояние, когда оно увеличивается ($\varepsilon > \xi$), либо когда оно уменьшается ($\varepsilon < \xi$);член уравнения $\frac{d^2\rho(x,t)}{dt^2}$ описывает случайное изменение состояния.

Сформулируем и решим для описания работы сети краевую задачу, учитывая ее перколяционные свойства. При числе блокированных узлов в сети $x = l$ она прекращает работу (l – величина порога перколяции сети). Поскольку мы стремимся избежать этого состояния, то необходимо, чтобы выполнялось условие $\rho(x, t)_{x=l} = 0$.

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 типа: $\rho(x, t)_{x=0} = 0$.

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

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

Используя методы операционного исчисления для плотности вероятности $\rho(x, t)$ обнаружения состояния системы в одном из значений на отрезке от 0 до l, можно решить данную краевую задачу и затем определить вероятность $Q_i(l, t)$ того, что порог перколяции l окажется к моменту времени t достигнутым или превзойденным:

$$Q(l,t) = 2e^{-\frac{2bx_0 + b^2 t}{4a}} \sum_{n=1}^{M} (-1)^{n+1} \frac{e^{\frac{bl}{2a}} \sin\left(\pi n \frac{x_0}{l}\right) + \sin\left(\pi n \frac{l - x_0}{l}\right)}{\pi n + \frac{b^2 l^2}{4\pi n a^2}} e^{-\frac{\pi^2 n^2 a t}{l^2}}, \qquad (7)$$

где M – число членов суммы ряда. В общем случае n принимает значения в сумме от 1 до бесконечности. Но поскольку ряд быстро сходится, то при численном вычислении суммы ряда в формуле (7) и моделировании можно принять M конечным (в нашем случае принято M = 1 000).

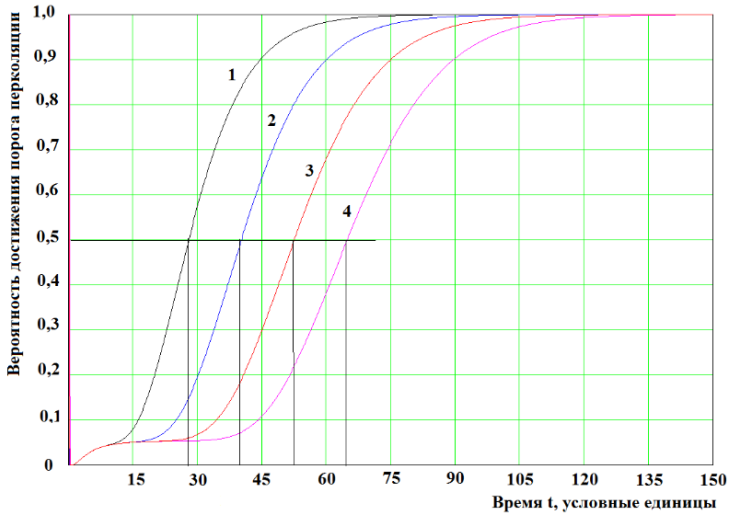

Рис. 4. Зависимость от времени значения вероятности достижения порога перколяции сети
Fig. 4. Time dependence of the probability of reaching the network percolation threshold

Проанализируем полученный результат. Возьмем произвольные значения x_0, ε и ξ ($\varepsilon > \xi$), например x_0 = 0,05, ε = 0,015 и ξ = 0,007. На рис. 4 представлена зависимость от времени вероятности

$Q_i(l, t)$ того, что к моменту времени t окажется достигнутым порог перколяции. Кривая *1* построена для значения порога перколяции сети $l_1 = 0{,}30$, кривая *2* для $l_2 = 0{,}40$, кривая *3* для $l_3 = 0{,}50$, кривая *4* для $l_4 = 0{,}60$.

Полученные результаты можно связать с результатами рассмотрения перколяционной модели. Пересечение горизонтальной линии на рис. 4, с кривыми линиями, описывающими поведение вероятностей, позволяет определить время достижения порога перколяции при заданных параметрах моделирования, а, следовательно, и потерю работоспособности 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

1. В сетях передачи данных могут происходить блокирование узлов, образование их кластеров и достижение 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 значений 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 динамическую задачу и определить необходимые для обеспечения заданного порога перколяции (надежность) величины коэффициентов в моделях, описывающих динамику блокирования узлов.

2. Модель распространения эволюционирующих вирусов в компьютерной сети может быть описана в графическом виде с помощью диаграммы возможных переходов между состояниями узлов, это позволяет получить систему кинетических дифференциальных уравнений, описывающих указанные процессы. В рамках модели любой узел сети может находиться в одном из трех состояний: в защищенном (иммунизированном), и узел сам может рассылать антивирусы (излечивает зараженные и иммунизирует свободные узлы); в зараженном (может рассылать копии вирусов по узлам сети); в нейтральном состоянии (может быть заражен). Анализ полученных решений показывает возможность существования в рамках модели различных режимов распространения вирусов; при некоторых наборах величин коэффициентов уравнений наблюдается осциллирующий характер вирусных эпидемий.

3. Разработанная на базе кинетических дифференциальных уравнений модель может быть модифицирована и расширена на основе создания 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, описываемый функцией любого вида.

4. При описании процесса блокирования узлов 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. Полученное дифференциальное уравнение позволяет сформулировать и решить краевую задачу изменения загруженности и блокировки сети. Взаимосвязь стохастической и перколяционной моделей позволяет оценить время достижения порога перколяции и потери работоспособности сети в целом.

5. 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, его доля должна находится в пределе от 0,48 (если блокируется 48% используемого оборудования, то все еще выполняется условие перколяции, так как доля неблокированных узлов равна 0,52) до 0,63 (превышать 48–63%).

ЛИТЕРАТУРА

1. Anderson H., Britton T. Stochastic Epidemic Models and Their Statistical Analysis. New-York : Springer, 2000. 140 p.
2. Bolker B.M., Earn D.J.D., Rohani P., Grenfell B.T. A simple model for complex dynamical transitions in epidemics // Science. 2000. V. 287. P. 667–670.
3. Wang C., Knight J.C., Elder M.C. On Viral Propagation and the Effect of Immunization // Proc. of 16th ACM Annual Computer Applications Conference. New Orleans, LA, 2000. P. 246–256.
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 // Proc. of ACM/SIGCOMM. 2000. P. 151–160.
5. Kumar M., Mishra B.K., Panda T.C. A new model on the spread of malicious objects in computer network // Int. J. of Hybrid Information Technology. 2013. V. 6, No. 6. P. 161–176.
6. Mishra B.K., Ansari G.M. Dierential epidemic model of virus and worms in computer network // Int. J. of Network Security. 2012. V. 14, No. 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 национального технического университета «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.
9. Chen L.-Ch., Carley K.M. The impact of countermeasure propagation on the prevalence of computer viruses // IEEE Transactions on Systems, Man, and Cybernetics. Part B: Cybernetics. 2004. V. 34, No. 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.
11. Vălean H., Pop A., Avram C. Intelligent model for virus spreading // The Int. Symposium on System Theory. Automation, Robotics, Computers, Informatics, Electronics and Instrumentation, 2007. 18–20 October. 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 J.R.C., Cesar F.B. Dynamical Models for Computer Viruses Propagation // Mathematical Problems in Engineering. 2008. V. 2008. Article ID 940526. 11 p. DOI: 10.1155/2008/940526.
14. Nazario J. Defense and detection strategies against internet worms. artech house. Boston–London : Artech House, 2004. 287 p.
15. Pastor-Satorras R., Vespignani A. Epidemics and Immunization in Scale-Free Networks // Handbook of Graphs and Networks: From the Genome to the Internet / S. Bornholdt, H.G. Schuster (eds.). Wiley-VCH, 2005. P. 111–130. DOI: 10.1002/3527602755.ch5.
16. Mizutaka S., Tanizawa T. Robustness analysis of bimodal networks in the whole range of degree correlation // Physical Review E. 2016. V. 94, is. 2. Article 022308.
17. De Brito J.B., Sampaio Filho C.I.N., Moreira A.A., Andrade J.S. Characterizing the intrinsic correlations of scale-free networks // Int. J. of Modern Physics C. 2016. V. 27, is. 3. Article. 1650024.
18. Timonin P.N. Statistical mechanics of high-density bond percolation // Physical Review E. 2018. V. 97, is. 5. Article number 052119.
19. Zhou A., Maletić S., Zhao Y. Robustness and percolation of holes in complex networks // Physica A: Statistical Mechanics and its Applications. 2018. V. 502. P. 459–468.
20. Katzav E., Biham O., Hartmann A.K. Distribution of shortest path lengths in subcritical Erdos-Rényi networks // Physical Review E. 2018. V. 98, is. 1. Article number 012301.
21. Hunt A.G., Yu F. The fractals of percolation theory in the geosciences (Book Chapter) // Fractals: Concepts and Applications in Geosciences. 2017. 1 Jan. P. 114–152.
22. Rubie D.C., Jacobson S.A. Mechanisms and Geochemical Models of Core Formation (Book Chapter) // Deep Earth: Physics and Chemistry of the Lower Mantle and Core. 2015. 1 Jan. P. 181–190.
23. Zhukov D., Khvatova T., Lesko S., Zaltsman A. Managing social networks: applying the Percolation theory methodology to understand individuals' attitudes and moods // Technological Forecasting and Social Change. 2018. V. 123. P. 234–245.
24. 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, is. 2. P. 90–97.

Поступила в редакцию 10 сентября 2019 г.

Lesko S.A., Zhukov D.O., Istratov L.A. (2020) MODELS OF DESCRIBING THE DYNAMICS OF BLOCKING NODES OF COMPUTER NETWORKS BY VIRUSES BASED ON THE USE OF PERCOLATION, KINETIC AND STOCHASTIC METHODS. *Vestnik Tomskogo gosudarstvennogo universiteta. Upravlenie, vychislitelnaja tehnika i informatika* [Tomsk State University Journal of Control and Computer Science]. 52. pp. 22–32

DOI: 10.17223/19988605/52/3

The paper presents a set of models describing the dynamics of blocking nodes of computer networks created on the basis of taking into account their percolation properties and blocking mechanisms (kinetic and stochastic). On the one hand, this model is based on

the use of percolation theory methods, which make it possible to determine the structural and informational characteristics of networks, such as the dependence of their percolation threshold on the average number of bonds per node (network density). On the other hand, dynamic processes of blocking the nodes and reaching the percolation threshold are considered. The percolation threshold is the minimum proportion of blocked nodes at which the entire network loses the properties of information transmission (there is no free path between any randomly selected nodes).

In the kinetic model, the processes of propagation in computer networks of evolving viruses in the course of obsolescence and delay of the action of antiviruses are considered. Further, on the basis of the graphical description of the possible transitions between the states of the nodes, systems of kinetic differential equations for the spread of viruses were obtained. Then using these equations and the percolation threshold value calculated by the network density, one can estimate the time of loss of its overall performance. Any network node can be in one of three states: in a protected (immunized) state, and it can itself send randomly (stochasticity) antiviruses (cures infected and immunizes free nodes) by selecting them in the address space; in the infected state (can send copies of viruses to network nodes); in a neutral state (may be infected). Analysis of the solutions obtained shows the possibility of the existence of various modes of spread of viruses. With some sets of values of the coefficients of differential equations, an oscillating pattern of the spread of viral epidemics is observed, which largely coincides with real observations. One of the advantages of the developed model is the possibility of its modification and expansion based on the creation of more complex graphical diagrams of state changes and transitions between them. In particular, it is possible to supplement the system of kinetic equations with a term that takes into account the general increase in the number of users and devices in computer networks over time.

A second-order differential equation was obtained in the model of stochastic dynamics of blocking nodes, based on a consideration of probability schemes for transitions between network states, and a boundary value problem was formulated, whose solution describes the dependence of the probability and time to reach the percolation threshold on the blocking probability of an individual network node. The percolation threshold itself is determined based on the density of the network.

Keywords: blocking network nodes; network percolation threshold; kinetic model of blocking nodes; stochastic dynamics of blocking nodes.

LESKO Sergey Aleksandrovich (Candidate of Physics and Mathematics, Russian Technological University (MIREA), Moscow, Russian Federation).
E-mail: sergey@testor.ru

ZHUKOV Dmitry Olegovich (Doctor of Technical Sciences, Russian Technological University (MIREA), Moscow, Russian Federation).
E-mail: zhukovdm@ya.ru

ISTRATOV Leonid Andreevich (Russian Technological University (MIREA), Moscow, Russian Federation).
E-mail: kuyahshtibov@gmail.com

REFERENCES

1. Anderson, H. & Britton, T. (2000) *Stochastic Epidemic Models and Their Statistical Analysis.* New-York: Springer, Verlag.
2. Bolker, B.M., Earn, D.J.D., Rohani, P. & Grenfell, B.T. (2000) A simple model for complex dynamical transitions in epidemics. *Science*. 287. pp. 667–670. DOI: 10.1126/science.287.5453.667
3. Wang, C., Knight, J.C. & Elder, M.C. (2000) On viral propagation and the effect of immunization. *Proc. of 16th ACM Annual Computer Applications Conference.* New Orleans, LA. pp. 246–256
4. Misra, V., Gong, W. & Towsley, D. (2000) A fluid based analysis of a network of AQM routers supporting TCP flows with an application to RED. *Proc. of ACM/SIGCOMM*. pp. 151–160. DOI: 10.1145/347059.347421
5. Kumar, M., Mishra, B.K. & Panda, T.C. (2013) A new model on the spread of malicious objects in computer network. *International Journal of Hybrid Information Technology*. 6(6). pp. 161–176. DOI: 10.14257/ijhit.2013.6.6.14
6. Mishra, B.K. & Ansari, G.M. (2012) Dierential epidemic model of virus and worms in computer network. *International Journal of Network Security*. 14(3). pp. 149–155. DOI: 10.1155/2008/940526
7. Semenov, S.G. & Davidov, V.V. (2012) Mathematical model of the spread of computer viruses in heterogeneous computer networks of automated process control systems. *Vestnik NTU "HPI*". 38. pp. 163–171.
8. Balthrop, J., Forrest, S., Newman, M.E.J. & Williamson, M.M. (2004) Technological networks and the spread of computer viruses. *Science.* 304. pp. 527–529. DOI: 10.1126/science.1095845
9. Chen, L.-Ch. & Carley, K.M. (2004) The impact of countermeasure propagation on the prevalence of computer viruses. *IEEE Transactions on Systems, Man, and Cybernetics. Part B: Cybernetics.* 34(2). pp. 823–833. DOI: 10.1109/tsmcb.2003.817098
10. Ojugo, A.A., Aghware, F.O., Yoro, R.E., Yerokun, M.O., Eboka, A.O., Anujeonye, C.N. & Efozia, F.N. (2015) Evolutionary model for virus propagation on networks. *Automation, Control and Intelligent Systems.* 3(4). pp. 56–62. DOI: 10.11648/j.acis.20150304.12
11. Vălean, H., Pop, A. & Avram, C. (2007) Intelligent model for virus spreading. *The International Symposium on System Theory. Automation, Robotics, Computers, Informatics, Electronics and Instrumentation*. 18-20. October. Craiova, Romania.
12. Delinger, Yu.M., Babanin, D.V. & Burkov, S.M. (2011) Mathematical models of the spread of viruses in computer networks of various structures. *Modelirovanie sistem – System Modeling*. 4(30). pp. 3–11.

13. Piqueira, J.R.C. & Cesar, F.B. (2008) Dynamical Models for Computer Viruses Propagation. *Mathematical Problems in Engineering*. 2008. Article ID 940526. DOI:10.1155/2008/940526
14. Nazario, J. (2004) *Defense and detection strategies against internet worms.* Artech House.
15. Pastor-Satorras, R. & Vespignani, A. (2005) *Epidemics and Immunization in Scale-Free Networks.* In: Bornholdt, S. & Schuster, H.G. (eds) *Handbook of Graphs and Networks: From the Genome to the Internet*. Wiley-VCH. DOI:10.1002/3527602755.ch5
16. Mizutaka, S. & Tanizawa, T. (2016) Robustness analysis of bimodal networks in the whole range of degree correlation. *Physical Review E*. 94(2). Article number 022308. DOI: 10.1103/PhysRevE.94.022308
17. De Brito, J.B., Sampaio Filho, C.I.N., Moreira, A.A. & Andrade, J.S. (2016) Characterizing the intrinsic correlations of scale-free networks. *International Journal of Modern Physics C*. 27(3). Article number 1650024. DOI: 10.1142/S0129183116500248
18. Timonin, P.N. (2018) Statistical mechanics of high-density bond percolation. *Physical Review E*. 97(5). Article number 052119. DOI: 10.1103/PhysRevE.97.052119
19. Zhou, A., Maletić, S. & Zhao, Y. (2018) Robustness and percolation of holes in complex networks. *Physica A: Statistical Mechanics and its Applications.* 502. pp. 459–468. DOI: 10.1016/j.physa.2018.02.149
20. Katzav, E., Biham, O. & Hartmann, A.K. (2018) Distribution of shortest path lengths in subcritical Erdos-Rényi networks. *Physical Review E*. 98(1). Article number 012301. DOI: 10.1103/PhysRevE.98.012301
21. Hunt, A.G. & Yu, F. (2017) The fractals of percolation theory in the geosciences. In: Ghanbarian, B. & Hunt, A.G. (eds) *Fractals: Concepts and Applications in Geosciences*. CRC Press. pp. 114–152.
22. Rubie, D.C. & Jacobson, S.A. (2015) Mechanisms and Geochemical Models of Core Formation. In: Terasaki, H. & Fischer, R. (eds) *Deep Earth: Physics and Chemistry of the Lower Mantle and Core*. pp. 181–190. DOI: 10.1002/9781118992487
23. Zhukov, D., Khvatova, T., Lesko, S. & Zaltsman, A. (2018) Managing social networks: applying the Percolation theory methodology to understand individuals' attitudes and moods. *Technological Forecasting and Social Change*. 123. pp. 234–245. DOI: 10.1016/j.techfore.2017.09.039
24. Zhukov, D.O., Khvatova, T.Yu., Lesko, S.A. & Zaltsman A.D. (2018) The influence of the connections density on clusterisation and percolation threshold during information distribution in social networks. *Informatika i ee primeneniya – Informatics and Applications*. 12(2). pp. 90–97. DOI: 10.14357/19922264180213