УДК 004.056.57

А.А. Бойко

СПОСОБ АНАЛИТИЧЕСКОГО МОДЕЛИРОВАНИЯ ПРОЦЕССА РАСПРОСТРАНЕНИЯ ВИРУСОВ В КОМПЬЮТЕРНЫХ СЕТЯХ РАЗЛИЧНОЙ СТРУКТУРЫ

Бойко А.А. **Способ аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры.**
Аннотация. Предложен способ аналитического моделирования процесса распространения вирусов в компьютерной сети. Он учитывает особенности сетевой структуры, поведенческие характеристики вирусов и подсистем защиты информации узлов и возможность исходного заражения множества узлов различными вирусами. Способ основан на представлении сети в виде модели с дискретными состояниями и временем переходов, которое распределено по обобщенному закону Эрланга *n*-го порядка.
Ключевые слова: распространение вирусов, компьютерная сеть, модель с дискретными состояниями и непрерывным временем, структура сети.

Boyko A.A. **Method of Analytical Modeling of Spread of Viruses in Computer Networks with Different Structures.**
Abstract. The article proposes a method of analytical modeling of viruses propagation process in computer network, which takes into account the characteristics of its topology, behavioral characteristics of viruses and information security sub-systems of nodes and likelihood of source infection of a plurality of nodes with different viruses. The method is based on performance of network topology in the form of a model with discrete states and times of branches, distributed by the generalized Erlang law of n-th order.
Keywords: the spread of virus, computer network, model with discrete states and continuum time, network structure.

1. Введение. При исследовании конфликта современных организационно-технических систем (например, конкурирующих промышленных предприятий или противоборствующих воинских формирований [1]) важно уметь оценивать их конфликтную устойчивость в условиях деструктивных информационно-технических воздействий [2] различного рода. Частной задачей такого исследования является оценка защищенности проектируемых или эксплуатируемых компьютерных сетей (далее – сетей) организационно-технических систем (ОТС) от воздействия вирусов на узловые информационно-технические средства (ИТС), образующие эти сети (далее – узлы). Информационно-техническими называются такие технические средства, которые участвуют в процессе создания и выполнения операций с данными, из которых может быть получена информация. ИТС является любое радиоэлектронное средство или средство вычислительной техники, комбинация таких средств друг с другом и (или) с другими видами технических средств [3].

Основными характерными чертами сетей конфликтующих ОТС с позиции распространения в них вирусов являются:

1) априорная ограниченность информации о составе программного и технического обеспечения узлов сетей;

2) фиксированная структура сетей, коррелирующая с иерархической структурой ОТС и включающая от десятков до тысяч узлов;

3) среднестатистические временные характеристики функционирования конкретных вирусов в узлах сетей ОТС, соответствующие вектору целей и возможностям этих вирусов;

4) среднестатистические временные характеристики функционирования подсистем защиты информации (ПЗИ) сетевых узлов, полученные из "инсайдерских" и открытых источников.

Очевидно, что оценка защищенности сетей ОТС от воздействия вирусов с применением натурных методов моделирования в подавляющем большинстве случаев является крайне дорогостоящей. Поэтому в настоящей статье уделяется внимание математическим моделям распространения вирусов в сетях ОТС.

2. Анализ существующих работ в области моделирования процесса распространения вирусов. На сегодняшний день известен весьма широкий спектр результатов отечественных и зарубежных исследований в области моделирования процесса распространения вирусов. В целях определения возможности их применения для анализа процесса распространения вирусов в сетях ОТС ограничимся упоминанием наиболее типовых из них.

Работы, посвященные анализу процесса распространения вирусов, традиционно делятся на два основных направления [4, 5]: аналитическое и имитационное.

Модели аналитического направления в свою очередь можно разделить на две группы. Модели первой группы (например, [4-14]) не учитывают структуру сетей, но предоставляют возможность для анализа важных с точки зрения вирусной угрозы состояний узлов с учетом времени. Исторически сложилось, что такие модели явились пионерскими в рассматриваемой области и были заимствованы из математических основ эпидемиологии. В этих моделях все множество объектов в зоне риска разделялось на несколько подмножеств "инфицированных", "уязвимых к заражению", "излеченных" и т.д., а динамика численности этих подмножеств описывалась дифференциальными уравнениями. Модели второй группы учитывают структуру сетей. Но они либо ограничены использованием заведомо недостаточного количества состояний узлов по причине высокой вычислительной сложности применяемых методов (например, [15-17]), либо не дают информа-

ции о состоянии защищенности каждого конкретного узла сети в заданный момент времени (например, [18]).

Одна из наиболее удачных классификаций моделей и систем имитационного направления представлена в [19]. Имитационные модели получили широкое применение в условиях появления высокопроизводительных систем имитационного моделирования, в том числе объектно-ориентированных (пример такой системы показан в [20]). Они обеспечивают высокую точность моделирования при большом количестве сетевых узлов. Однако такие модели требуют детального знания алгоритмов информационного взаимодействия узлов сети, которые зачастую являются недоступными для исследователя.

Для наиболее вероятных на практике исходных данных только о структуре сетей взаимодействующих ОТС и среднестатистических временных характеристиках функционирования вирусов и ПЗИ [21, 22] их узлов приоритет имеют аналитические модели. Они отличаются высокой скоростью моделирования и возможностью получения решения «в общем виде» [5]. Однако попытки применения известных аналитических моделей процесса распространения вирусов или их комбинаций для потенциально доступного набора исходных данных о сетях ОТС оказались безуспешными, поскольку преимущества этих моделей с лихвой перекрывались их недостатками. В результате возникла потребность в разработке нового подхода, парирующего недостатки известных аналитических моделей в рассматриваемой области.

Цель работы – *разработка способа аналитического моделирования процесса распространения вирусов в сетях различной структуры, позволяющего в различные моменты времени оценить вероятность заражения несколькими вирусами каждого узла этих сетей с учетом поведенческих характеристик вирусов и подсистем защиты информации узлов.*

3. Математическая модель процесса распространения вирусов в компьютерных сетях различной структуры. Пусть сеть состоит из N узлов и в различные моменты времени заражается V типами вирусов по q_v экземпляров с различными вероятностями изначального заражения μ_g (g=1..q_v). Структура сети задается среднестатистическими временными интервалами (далее – интервалами) τ_{ij} с момента штатного инициирования i-м узлом сеанса связи с j-м узлом до момента окончания этого сеанса. Вирусы могут обеспечивать и не обеспечивать скрытность своего распространения (далее – скрытные и не скрытные вирусы, соответственно). Скрытному вирусу, находящемуся в i-м узле, для заражения j-го узла необходимо дождаться штатного сеанса связи между i-м и j-м узлами. Не скрытный вирус, попав в i-й узел, присту-

пает к инициированию сеанса связи с *j*-м узлом независимо от штатных сеансов связи.

Тогда временная диаграмма заражения *j*-го узла вирусом *v*-го типа, находящимся в *i*-м узле, имеет вид, показанный на рисунке 1. В точке 1 на временной оси вирус внедрился в *i*-й узел и начинает подготовку к размножению. Вирус готов к размножению из *i*-го узла в точке 3. От точки 3 до точки 5 вирус внедряется из *i*-го в *j*-й узел. ПЗИ *i*-го узла стремится излечить вирус. Излечивание начинается с точки 1 и, в зависимости от возможностей ПЗИ, заканчивается либо в точках 2 (вариант 1) или 4 (вариант 2) и тогда вирус не сможет размножиться, либо в точке 6 (вариант 3) и тогда вирус размножится. По причине информационной несовместимости вирус может не внедриться в узел. Например, вирус "не знает" протоколы взаимодействия узлов или их уязвимости.

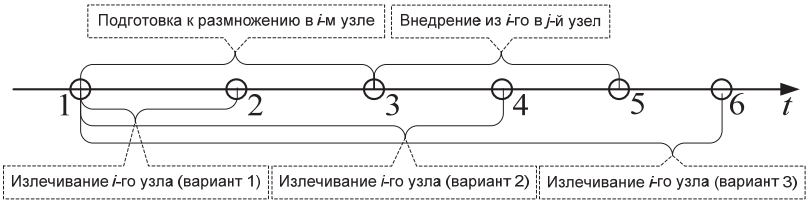

Рис. 1. Временная диаграмма заражения вирусом узла сети

Значение интервала передачи вируса *v*-го типа между связанными *i*-м и *j*-м узлами предлагается вычислять по формуле:

$$m_{vij} = \begin{cases} \alpha_{vij} + \beta_{vi}, \text{ если } \gamma_{vi} > \alpha_{vij} + \beta_{vi}; \\ \infty, \text{ если вирус информационно не совместим} \\ \text{с узлом или } \gamma_{vi} \le \alpha_{vij} + \beta_{vi}, \end{cases} \quad (1)$$

где α_{vij} – интервал с момента готовности вируса *v*-го типа к размножению в *i*-м узле до момента его внедрения в *j*-й узел; β_{vi} – интервал с момента внедрения вируса *v*-го типа в *i*-й узел до момента, когда этот вирус будет готов к размножению; γ_{vi} – интервал с момента внедрения вируса *v*-го типа в *i*-й узел до момента, когда данный узел от этого вируса будет излечен.

Рассмотрим, каким образом можно получить численные значения показателей α_{vij}, β_{vi} и γ_{vi} в формуле (1).

Сеансы связи между парой связанных узлов сети могут устанавливаться либо по инициативе только одного из них (например, в большинстве пар "клиент-сервер" сеансы связи инициируются только кли-

ентами), либо по инициативе любого узла из этой пары (например, в паре связанных сетевых терминалов сеанс связи может инициировать любой из них). Поскольку скрытный вирус может передаваться независимо от того, какой из двух связанных узлов является инициатором сеанса связи, значение интервала α_{vij} предлагается вычислять как:

$$\alpha_{vij} = \begin{cases} \dfrac{1}{1/\tau_{ij} + 1/\tau_{ji}} = \dfrac{\tau_{ij} \cdot \tau_{ji}}{\tau_{ij} + \tau_{ji}}, \text{если связь инициируется} \\ \text{обоими узлами и вирус скрытный;} \\ \tau_{ij}, \text{ если связь инициируется только одним узлом} \\ \text{и вирус скрытный;} \\ \tau_{v}, \text{ если вирус не скрытный,} \end{cases} \quad (2)$$

где τ_v – интервал внедрения не скрытного вируса v-го типа, одинаковый для всех узлов сети и являющийся исходной поведенческой характеристикой вирусов этого типа.

Поведенческие характеристики вирусов рассмотрены в работах [21, 22]. В этих работах анализируется информационный конфликт ПЗИ ИТС со специальными программными средствами (СПС), частным случаем которых являются вирусы. В таком конфликте СПС находится в трех основных режимах функционирования: подготовка к применению, скрытое и открытое применение, а ПЗИ выполняет типовые задачи по предупреждению, обнаружению и устранению последствий воздействия СПС. Полагая отлаженными процессы сопряжения узлов в сети друг с другом, этот конфликт с позиции распространения вирусов в сетях сводится к частному конфликту вируса и ПЗИ узла, граф состояний которого представлен на рисунке 2.

Состояния на рисунке 2 характеризуют поведенческие характеристики вируса и ПЗИ узла и имеют следующее описание:

A_1 – вирус внедрился в программную среду узла и анализирует его текущее состояние;

A_2 – вирус производит отказ в обслуживании узла, приводящий к невозможности выполнения любых задач;

A_3 – вирус использует функции узла в своих целях;

A_4 – вирус осуществляет вывод узла из строя;

A_5 – вирус размножается;

A_6 – вирус дезинформирует узел;

A_7 – вирус производит разведку;

A_8 – ПЗИ проводит принудительный поиск вирусов;

A_9 – вирус осуществляет самомодификацию;
A_{10} – вирус перешел в режим ожидания;
A_{11} – вирус излечен.

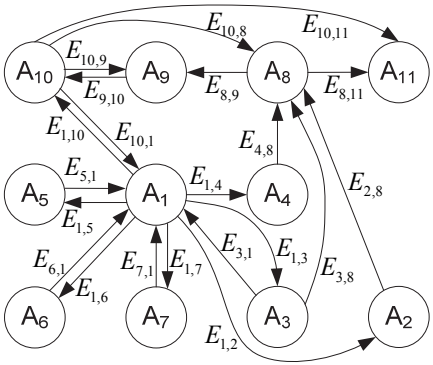

Рис. 2. Граф состояний динамики конфликта вируса и ПЗИ узла

Значения интервалов переходов конфликта вируса и ПЗИ для каждого узла могут быть получены натурным методом, задаваться экспертно или вычисляться с использованием специальных методик. Значение показателя β_{vi} по существу равно значению интервала $E_{1,5}$ перехода i-го узла из состояния A_1 в состояние A_5 и является исходной поведенческой характеристикой вируса v-го типа. Интервал γ_{vi} соответствует интервалу перехода рассматриваемого конфликта i-го узла из состояния A_1 в состояние A_{11} при воздействии вируса v-го типа. Поэтому численное значение этого интервала предлагается вычислять следующим образом.

Интервалы переходов конфликта вируса и ПЗИ узла из одного состояния в другое не имеют экспоненциальный характер, а коррелируют с некоторой средней величиной. Для анализа такого конфликта применим метод аналитического описания процессов с дискретным множеством состояний и не показательными распределениями времен переходов [23]. Сущность данного метода состоит в преобразовании структуры дискретного процесса с распределенными по обобщенному закону Эрланга n-го порядка временем переходов в непрерывную марковскую цепь путем введения псевдосостояний. Полученный процесс конфликтного взаимодействия описывается в виде системы обыкновенных линейных дифференциальных уравнений. Данный метод оперирует тем фактом, что произвольная плотность распределения времени нахождения системы в некотором состоянии с достаточной степенью точности аппроксимируется с помощью обобщенного закона Эр-

ланга n-го порядка [24]. На практике 2-й или 3-й порядки этого закона являются достаточными для исследования моделей рассматриваемого класса [21-23]. Полученный с применением метода [23] граф марковской цепи конфликта вируса и ПЗИ узла при n=2 имеет 165 псевдосостояний и 990 переходов, а при n=3 – 2 305 псевдосостояний и 15 689 переходов. Поэтому в настоящей статье эти графы не приводятся.

С учетом изложенного значение показателя γ_{vi} может быть получено с применением следующего алгоритма:

1) решение задачи Коши для марковской цепи конфликта вируса v-го типа и ПЗИ в j-м узле численным методом. Начальным условием является равенство единице вероятности нахождения процесса в состоянии A_1 и нулевые вероятности других состояний;

2) вычисление значения показателя γ_{vi} как интервала времени с момента, когда конфликт вируса и ПЗИ вышел из состояния A_1, до момента, когда этот конфликт перешел в состояние A_{11}, с учетом того, что изображенный на рисунке 2 процесс не является стационарным:

$$\gamma_{vi} = t\{P_{i11} = \xi_{i11} - \Delta\} - t\{P_{i1} = \xi_{i1} - \Delta\}, \qquad (3)$$

где $t\{P_{i11}=\xi_{i11}-\Delta\}$ – момент времени установления в i-м узле процесса конфликта вируса и ПЗИ в состоянии A_{11} с вероятностью $\xi_{i11}-\Delta$; $t\{P_{i1}=\xi_{i1}-\Delta\}$ – момент времени, после которого процесс конфликта вируса и ПЗИ для i-го узла находится в состоянии A_1 с вероятностью меньше $\xi_{i1}-\Delta$; Δ – погрешность численного метода решения задачи Коши; ξ_{i1} и ξ_{i11} – достаточные вероятности нахождения процесса конфликта вируса и ПЗИ i-го узла в состояниях A_1 и A_{11}, соответственно.

Поскольку рассматриваемая математическая модель оперирует среднестатистическими временными интервалами, то показатели ξ_{i1} и ξ_{i11} в формуле (3) предлагается определять как вероятности нахождения процесса конфликта вируса и ПЗИ в состояниях A_1 и A_{11} в т.н. "медианный" момент времени. "Медианным" будем называть момент времени, в котором площадь, ограниченная кривой распределения вероятности соответствующего состояния, делится пополам.

Полученные таким образом значения интервалов передачи вирусов между связанными узлами предлагается использовать для анализа процесса распространения вирусов в сетях различной структуры с применением указанного выше универсального метода [23]. Для этого состояния процесса распространения вирусов будем отождествлять с узлами сети, а переходы между состояниями – со связями между этими узлами. Такое отождествление уместно для наиболее часто встречающегося на практике случая, когда ПЗИ узлов запоминают излеченные ими вирусы, приобретая тем самым иммунитет к ним.

4. Содержание способа аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры. Исходными данными для способа являются:

– количество узлов сети (N);

– интервалы с момента инициирования узлами соединений до момента окончания этих соединений (τ_{ij});

– количество типов вирусов (V);

– количество экземпляров вируса каждого типа (q_v);

– вероятности изначального заражения сети различными экземплярами вирусов (μ_g);

– интервалы внедрения не скрытных вирусов (τ_v);

– поведенческие характеристики вирусов и ПЗИ в каждом узле сети, обусловливающие интервалы переходов (E_{vjsl}, где s и l – индексы переходов модели конфликта вируса v-го типа и ПЗИ j-го узла);

– интервал моделирования (T_0);

– точность численного метода решения задачи Коши (Δ).

Предлагаемый способ состоит в выполнении следующих шагов.

Шаг 1. Вычисление γ_{vi} с применением вышеуказанного алгоритма для каждого узла сети и каждого типа вируса.

Шаг 2. Представление сети в виде ориентированного графа, в котором переходы характеризуются интервалами m_{vij}, вычисляемыми по формуле (1).

Шаг 3. Преобразование построенного на шаге 2 графа в марковскую цепь с использованием метода [23].

Шаг 4. Вычисление вероятностно-временных характеристик заражения всех узлов сети всеми экземплярами вирусов всех типов. Для этого для построенной на шаге 3 марковской цепи решается задача Коши для каждого экземпляра каждого вируса.

Начальные условия для решения задачи Коши:

– единичная вероятность нахождения экземпляра вируса в том узле, который этим вирусом заражен изначально, и нулевые вероятности нахождения этого экземпляра вируса в остальных узлах;

– начальное время соответствует времени начала действия экземпляра вируса.

Шаг 5. Определение вероятностно-временной характеристики заражения каждого i-го узла вирусом каждого v-го типа по формуле:

$$P_{vi}(t) = \max_{g=1..q_v} \left\{ P_{gi}(t) \cdot \mu_g \right\}, \qquad (4)$$

где $P_{gi}(t)$ – вероятностно-временная характеристика заражения i-го узла g-м экземпляром вируса v-го типа; μ_g – вероятность изначального заражения сети g-м экземпляром вируса v-го типа.

5. Пример применения способа. Рассмотрим пример сети с 7 узлами, граф которой представлен на рисунке 3.

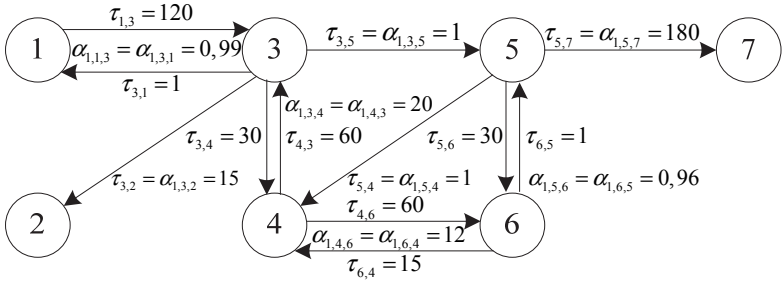

Рис. 3. Граф сети

Сеть поражается четырьмя вирусами двух типов. Узел 1 в начальный момент времени и узел 5 через сутки после этого заражаются скрытным вирусом (1-й тип). Узел 3 через 6 часов после начального момента и узел 6 через 12 часов заражаются не скрытным вирусом (2-й тип). Значения интервалов τ_{ij} и α_{1ij} для вирусов 1-го типа приведены на рисунке 3 в минутах. Для вирусов 2-го типа τ_v = 1 мин. Все узлы кроме узла 4 имеют одинаковый состав программного и информационного обеспечения. Вирусы 1-го и 2-го типов "знают" уязвимости в протоколах информационного взаимодействия всех узлов сети кроме узла 4. Исходные данные о конфликте вирусов 1-го типа и ПЗИ имеют вид: $E_{1,i,1,2}=E_{1,i,1,3}=E_{1,i,1,5}=E_{1,i,1,6}=E_{1,i,1,7}$ = 3 часа; $E_{1,i,1,4}$ = 2 нед; $E_{1,i,1,10}=E_{1,i,6,1}=$ $=E_{1,i,7,1}=E_{1,i,9,10}$=1 мин; $E_{1,i,2,8}=E_{1,i,10,1}$=30 мин; $E_{1,i,3,1}=E_{1,i,8,11}$=1 час; $E_{1,i,3,8}=$ $=E_{1,i,4,8}$ = 15 мин; $E_{1,i,5,1}$ = 12 час; $E_{1,i,8,9}=E_{1,i,10,8}=E_{1,i,10,9}=E_{1,i,10,11}$ = 1 день. Исходные данные о конфликте вирусов 2-го типа и ПЗИ имеют вид: $E_{2,i,1,2}=E_{2,i,1,3}=E_{2,i,1,5}=E_{2,i,1,6}=E_{2,i,1,7}=E_{2,i,3,1}=E_{2,i,5,1}=E_{2,i,8,11}=E_{2,i,10,1}$ = 15 мин; $E_{2,i,1,4}$= 1 нед; $E_{2,i,1,10}=E_{2,i,9,10}$= 1 мин; $E_{2,i,2,8}=E_{2,i,3,8}=E_{2,i,4,8}$ = 10мин; $E_{2,i,6,1}$ = $=E_{2,i,10,8}$ = 60мин; $E_{2,i,7,1}$ = 30мин; $E_{2,i,8,9}=E_{2,i,10,9}$ = 1день; $E_{2,i,10,11}$ = 3часа. Поведенческие характеристики ПЗИ учитывают не скрытный характер вирусов 2-го типа. Интервал моделирования T_0 равен 3 месяцам.

Из исходных данных видно, что β_{1i}=3часа, а β_{2i}=15мин. Полученные для них значения показателей γ_{1i} и γ_{2i} составляют десятки дней и практически не оказывают влияние на процесс распространения вирусов. Для обобщенного закона Эрланга при n=2 анализируемая сеть имеет 25 псевдосостояний и 58 переходов, а при n=3 она имеет 67 псевдосостояний и 176 переходов. Результирующие вероятностно-временные характеристики заражения узлов сети совокупностью вирусов одного типа показаны на рисунке 4.

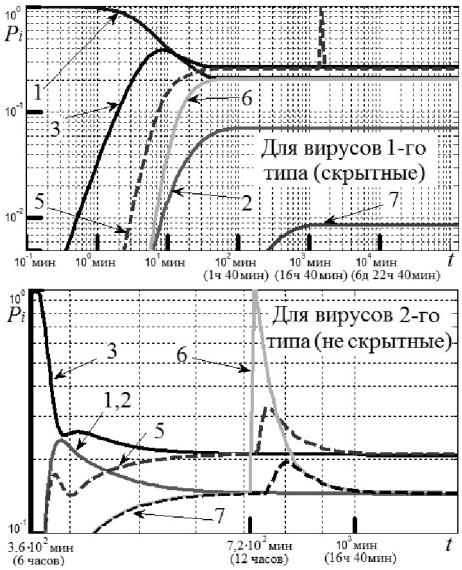

Рис. 4. Вероятностно-временные характеристики заражения узлов сети совокупностью вирусов одного типа

Полученные с использованием предложенного способа вероятностно-временные характеристики могут применяться, в частности, для оценки количества узлов сети, зараженных вирусом каждого типа. Для этого вводится пороговое значение, относительно которого принимается решение о том, заражен ли вирусом узел или нет. Пример таких зависимостей приведен на рисунке 5. В нем пороговое значение равно усредненной на интервале моделирования вероятности заражения вирусом соответствующего типа наименее зараженного узла сети.

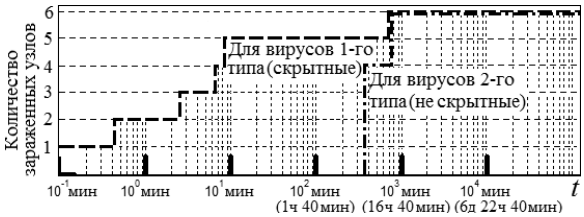

Рис. 5. Зависимость количества зараженных вирусами узлов от времени

Зависимости на рисунке 5 свидетельствуют о том, что для указанных исходных данных ПЗИ вирусы 1-го типа уже через 8 минут

способны заразить 5 из 7 узлов сети, а вирусы 2-го типа в течение 1 часа могут заразить все 6 доступных для них узлов.

6. Заключение. Предложенный способ предоставляет возможность для аналитического решения задачи оценки вероятности заражения каждого узлового информационно-технического средства компьютерной сети несколькими экземплярами вирусов одного или нескольких типов в различные моменты времени. Способ основан на представлении сети в виде модели с дискретными состояниями и распределенным по обобщенному закону Эрланга n-го порядка временем переходов. Он учитывает особенности структуры компьютерных сетей и известные из практики поведенческие характеристики вирусов и подсистем защиты информации узловых информационно-технических средств. Способ может быть применен для исследования конфликтной устойчивости сложных организационно-технических систем.

Литература

1. *Бойко А.А., Храмов В.Ю.* Модель информационного конфликта информационно-технических и специальных программных средств в вооруженном противоборстве группировок со статичными характеристиками // Радиотехника. 2013. №7. С. 5-10.
2. *Бойко А.А.*, *Дьякова А.В.* Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств // Информационно-управляющие системы. 2014. № 3. С. 84-92.
3. *Балыбин В.А., Донсков Ю.Е., Бойко А.А.* О терминологии в области радиоэлектронной борьбы в условиях современного информационного противоборства // Военная Мысль. 2013. № 9. С. 28–32.
4. *Кондратьев М.А.* Методы прогнозирования и модели распространения заболеваний // Компьютерные исследования и моделирование. 2013. Т. 5. № 5. С. 863-882.
5. *Котенко И.В., Воронцов В.В.* Аналитические модели распространения сетевых червей // Труды СПИИРАН. 2007. № 4. С. 208-224.
6. *Zhang C., Feng T., Zhao Y., Jiang G.* A New Model for Capturing the Spread of Computer Viruses on Complex-Networks // Discrete Dynamics in Nature and Society. 2013. vol. 2013. 9 p.
7. *Mishra B.K., Jha N.* SEIQRS model for the transmission of malicious objects in computer network // Applied Mathematical Modelling. 2010. vol. 34. no. 3. pp. 710–715.
8. *Gan C., Yang X., Liu W., Zhu Q.* A propagation model of computer virus with nonlinear vaccination probability // Communications in Nonlinear Science and Numerical Simulation. 2014. vol. 19. no. 1. pp. 92–100.
9. *Wang Y., Jin Z., Yang Z., Zhang Z.-K., Zhou T., Sun G.-Q.* Global analysis of an SIS model with an infective vector on complex networks // Nonlinear Analysis: Real World Applications. 2012. vol.13. no.2. pp.543–557.
10. *Piqueira J.R.C., Navarro B.F., Monteiro L.H.A.* Epidemiological Models Applied to Viruses in Computer Networks // Journal of Computer Science. 2005. no. 1(1). pp. 31-34.

11. *Толстых Н.Н., Остапенко А.Г., Толстых И.О., Ахромеев М.В.* Распространение вирусов в кластеризованной сети мобильной связи // Информация и безопасность. 2008. № 3. С. 441-444.
12. *Гусаров А.Н., Жуков Д.О., Косарева А.В.* Описание динамики распространения компьютерных угроз в информационно-вычислительных сетях с запаздыванием действия антивирусов // Вестник МГТУ им. Н.Э. Баумана. Сер. "Приборостроение". 2010. № 1. С. 112-120.
13. *Климентьев К.Е.* Моделирования распространения и взаимодействия самовоспроизводящихся объектов // Известия Самарского научного центра Российской академии наук, 2014. т. 16. № 4(2), С. 313-317.
14. *Madar N., Kalisky T., Cohen R., ben-Avraham D., Havlin S.* Immunization and epidemic dynamics in complex networks // The European Physical Journal B. 2004. № 38. pp. 269-276.
15. *Новиков С.В.* Модель распространения вирусных атак в сетях передачи данных общего пользования на основе расчета длины гамильтонова пути: автореф… дис. канд. техн. наук // СПб: СПб ГУ ИТМО, 2007.
16. *Далингер Я.М., Бабанин Д.В., Бурков С.М.* Математические модели распространения вирусов в компьютерных сетях различной структуры // Информатика и системы управления. 2012. № 3(33). С. 25-33.
17. *Semenov S.G., Davydov V.V.* A Mathematical Model for Technology for Spreading Malicious Software across Heterogeneous Networks based on Markov Chains // European researcher. 2014. № 1-1 (66). pp. 21-30.
18. *Утакаева И.Х.*, *Кунижева Л.А.* Математическая модель распространения вирусов в сети на предфрактальных графах // Информационное противодействие угрозам терроризма. 2012. №18. С. 64-70.
19. *Котенко И.В., Воронцов В.В., Уланов А.В.* Модели и системы имитационного моделирования распространения сетевых червей // Труды СПИИРАН. 2007. № 4. С. 225-238.
20. *Котенко И.В., Шоров А.В.* Механизмы защиты компьютерных сетей от инфраструктурных атак на основе биоинспирированного подхода «нервная система сети» // Вопросы защиты информации. 2013. № 2. С. 57-66.
21. *Бойко А.А.* Способ стратифицированного аналитического описания процесса функционирования информационно-технических средств // Информационные технологии. 2015. № 1. С. 35-42.
22. *Бойко А.А., Будников С.А.* Модель информационного конфликта специального программного средства и подсистемы защиты информации информационно-технического средства // Радиотехника. 2015. №4. С. 136-141.
23. *Чикин М.Г.* Метод аналитического описания процессов с дискретным множеством состояний и не показательными распределениями времен переходов // Информационно-измерительные и управляющие системы. 2004. №5. С. 8-11.
24. *Кокс Д., Смит В.* Теория восстановления // М.: Сов. радио, 1967. 300 с.

References

1. Boyko A.A., Khramov V.U. [Model of Information Conflict between Special Software and Information-Technical Tools in Military Warfare with Static Characteristics]. *Radiotekhnika - Radioengineering*. 2013. no. 7. pp. 5-10. (In Russ.).
2. Boyko A.A., Djakova A.V. [Method of Developing Test Remote Information-Technical Impacts on Spatially Distributed Systems of Information-Technical Tools] . *Informatsionno-Upravliaiushchie Sistemy - Information and Control Systems*. 2014. no. 3. pp. 84-92. (In Russ.).

3. Balybin V.A., Donskov Ju.E., Boyko A.A. [About the terminology in the field of electronic warfare in modern information warfare]. *Voennaja Mysl' - Military Thought*. 2013. no. 9. pp. 28–32. (In Russ.).
4. Kondrat'ev M.A. [Forecasting methods and models of disease]. *Komp'juternye issledovanija i modelirovanie - Computer research and modeling*. 2013. vol. 5. no. 5. pp. 863–882. (In Russ.).
5. Kotenko I.V., Voroncov V.V. [Analytical models of network worm propagation]. *Trudy SPIIRAN - SPIIRAS Proceedings*. 2007. no. 4. pp. 208-224. (In Russ.).
6. Zhang C., Feng T., Zhao Y., Jiang G. A New Model for Capturing the Spread of Computer Viruses on Complex-Networks. *Discrete Dynamics in Nature and Society*. 2013. vol. 2013. 9 p.
7. Mishra B.K., Jha N. SEIQRS model for the transmission of malicious objects in computer network. *Applied Mathematical Modelling*. 2010. vol. 34. no. 3. pp. 710–715.
8. Gan C., Yang X., Liu W., Zhu Q. A propagation model of computer virus with nonlinear vaccination probability. *Communications in Nonlinear Science and Numerical Simulation*. 2014. vol. 19. no. 1. pp. 92–100.
9. Wang Y., Jin Z., Yang Z., Zhang Z.-K., Zhou T., Sun G.-Q. Global analysis of an SIS model with an infective vector on complex networks. *Nonlinear Analysis: Real World Applications*. 2012. vol.13. no.2. pp.543–557.
10. Piqueira J.R.C., Navarro B.F., Monteiro L.H.A. Epidemiological Models Applied to Viruses in Computer Networks. *Journal of Computer Science*. 2005. no. 1(1). pp. 31-34.
11. Tolstyh N.N., Ostapenko A.G., Tolstyh I.O., Ahromeev M.V. [The spread of viruses in a clustered mobile network]. *Informacija i bezopasnost' - Information and security*. 2008. no. 3. pp. 441-444. (In Russ.).
12. Gusarov A.N., Zhukov D.O., Kosareva A.V. [Description of the dynamics of the spread of computer threats in the information and computer networks with delay action antivirus]. *Vestnik MGTU im. N.Je. Baumana. Ser. "Priborostroenie" - Herald of the Bauman Moscow State Technical University. Insrtument Engineering*. 2010. no. 1. pp. 112-120. (In Russ.).
13. Kliment'ev K.E. [Modeling of the propagation and interaction of self-replicating objects]. *Izvestija Samarskogo Nauchnogo Centra Rossijskoj Akademii Nauk - Izvestiya of Samara scientific center of the Russian Academy of Sciences*. 2014. vol. 16. no. 4(2). pp. 313-317. (In Russ.).
14. Madar N., Kalisky T., Cohen R., ben-Avraham D., Havlin S. Immunization and epidemic dynamics in complex networks. *The European Physical Journal B*. 2004. no. 38. pp. 269-276.
15. Novikov S.V. *Model' rasprostranenija virusnyh atak v setjah peredachi dannyh obshhego pol'zovanija na osnove rascheta dliny gamil'tonova puti* [Model the spread of viral attacks in networks of public data by calculating the length of a Hamiltonian path]. *synopsis... dis. cand. tech. sciences*. St. Petersburg. GU ITMO. 2007. 17 p. (In Russ.).
16. Dalinger Ja.M., Babanin D.V., Burkov S.M. [Mathematical models of virus spreading in multicomputer systems with different structures]. *Informatika i sistemy upravlenija - Information science and control systems*. 2012. no. 3(33). pp. 25-33. (In Russ.).
17. Semenov S.G., Davydov V.V. A Mathematical Model for Technology for Spreading Malicious Software across Heterogeneous Networks based on Markov Chains. *European researcher*. 2014. no. 1-1 (66). pp. 21-30. (In Russ.).
18. Utakaeva I.H., Kunizheva L.A. [A mathematical model of the spread of viruses on the network on prefractal graphs]. *Informacionnoe protivodejstvie ugrozam terrorizma - Counteracting the threats of terrorism*. 2012. no. 18. pp. 64-70. (In Russ.).

19. Kotenko I.V., Voroncov V.V., Ulanov A.V. [Models and systems of network worm propagation simulation]. *Trudy SPIIRAN - SPIIRAS Proceedings*. 2007. no. 4. pp. 225-238. (In Russ.).
20. Kotenko I.V., Shorov A.V. [Infrastructure attack protection mechanisms based on bio-inspired approach "Network Nervous System"]. *Voprosy zashhity informacii - Information security questions*. 2013. no. 2. pp. 57-66. (In Russ.).
21. Boyko A.A. [Method of Stratified Analytical Description of the Process of Functioning of Information-Technical Tools]. *Informacionnye tehnologii - Information Technologies*. 2015. no. 1. pp. 35-42. (In Russ.).
22. Boyko A.A., Budnikov S.A. [Model of information conflict between special software and information security subsystem of information-technical tool]. *Radiotekhnika - Radioengineering*. 2015. no. 4. pp. 136-141. (In Russ.).
23. Chikin M.G. [Method of analytical description of processes with a discrete set of states and exponential distributions of times of transitions]. *Informacionno-izmeritel'nye i upravljajushhie sistemy - Information-measuring and Control Systems*. 2004. no. 5. pp. 8-11. (In Russ.).
24. Koks D., Smit V. *Teorija vosstanovlenija* [The theory of recovery]. M.: Sov. radio, 1967. 300 p. (In Russ.).

Бойко Алексей Александрович — к-т тех. наук, доцент, зам. начальника отдела, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: методы и системы защиты информации, методы оценки качества сложных систем. Число научных публикаций — 100. algeminy@mail.ru; ВУНЦ ВВС "ВВА", ул. Ст. Большеви хъков, д. 54А, г. Воронеж, 394064, РФ; р.т. +7(473)236-5228, факс +7(473)244-7860.

Boyko Aleksey Aleksandrovich — Ph.D., Tech., associate professor, associate chief of department, Military education-science center of Military aviation forces “Military aviation academy named for prof. N.E. Zhukovsky and J.A. Gagarin” (Voronezh, Russian Federation). Research interests: methods and systems of information protection, methods of assessing the quality of complex systems. The number of publications — 100. algeminy@mail.ru; MESC MAF "MAA", 54A, Old Bolsheviks street, Voronezh, 394064, Russia; office phone +7(473)236-5228, fax +(473)244-7860.

РЕФЕРАТ

Бойко А.А. **Способ аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры.**

Предложен способ аналитического моделирования процесса распространения вирусов в компьютерной сети. Он учитывает особенности сетевой структуры, поведенческие характеристики вирусов и подсистем защиты информации узлов и возможность исходного заражения множества узлов различными вирусами.

Способ основан на представлении сети в виде модели с дискретными состояниями и временем переходов, распределенным по обобщенному закону Эрланга *n*-го порядка. В модели состояния процесса распространения вирусов отождествляются с узлами сети, а переходы между состояниями – со связями между этими узлами. Полученная модель процесса распространения вирусов преобразуется в непрерывную марковскую цепь путем введения псевдосостояний. Результирующая марковская цепь описывается в виде системы обыкновенных линейных дифференциальных уравнений.

Поведенческие характеристики вирусов и подсистем защиты информации узлов определяются следующими состояниями: вирус производит отказ в обслуживании, приводящий к невозможности выполнения любых задач; вирус использует функции узла в своих целях; вирус осуществляет вывод узла из строя; вирус размножается; вирус дезинформирует узел; вирус производит разведку; подсистема защиты информации узла проводит принудительный поиск вирусов; вирус осуществляет самомодификацию; вирус перешел в режим ожидания; вирус излечен.

Способ применим для случая, когда подсистемы защиты информации узлов запоминают излеченные ими вирусы, приобретая тем самым иммунитет к ним. Он может быть использован при исследовании конфликтной устойчивости сложных организационно-технических систем в условиях деструктивных информационно-технических воздействий.

SUMMARY

Boyko A.A. **Method of Analytical Modeling of Spread of Viruses in Computer Networks with Different Structures.**

The article proposes a method of analytical modeling of the spread of viruses in computer networks. It takes into account the characteristics of the network structure, behavioral characteristics of viruses and information security subsystems of hosts and the possible source of infection of many hosts with different viruses.

The method is based on representing the network in the form of a model with discrete states and transitions, distributed by the generalized Erlang law of n-th order. In the model, the states of the process of viruses spreading are identified with the hosts of the network, and transitions between states - with connections between these hosts. The resulting model of the spread of viruses is converted to a continuous Markov chain by introducing pseudostates. The resulting Markov chain is described as a system of ordinary linear differential equations.

Behavioral characteristics of viruses and information security subsystems of hosts are determined by the following conditions: the virus produces a denial of service, resulting in the inability of the host to perform any task; the virus uses the functions of the host for its own purposes; the virus disables the host; the virus replicates; the virus misinforms the host; the virus produces intelligence; the infomation security subsystem of host conducts forcible virus search; the virus carries out self-modification; the virus has passed in the standby mode; the virus is cured.

The method is applicable for the case when information security subsystems of hosts remember cured viruses, thereby acquiring immunity to them. It can be used in the study of conflict stability of complex organizational-technical systems in terms of destructive information-technical influences.