УДК 621.396.253

А.А. Смирнов, И.А. Березюк, Мохамад Абу Таам Гани

Кировоградский национальный технический университет, Кировоград

СТРУКТУРНО-ЛОГИЧЕСКАЯ GERT-МОДЕЛЬ ТЕХНОЛОГИИ РАСПРОСТРАНЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Разработана структурно-логическая GERT-модель технологии распространения компьютерных вирусов, позволившая получить аналитическое выражение для расчета эквивалентной W-функции времени распространения в информационно-телекоммуникационных системах наиболее опасных компьютерных вирусов типа Flame с конечными результатами лечения и иммунизации узлов информационно-телекоммуникационных систем, а также выхода телекоммуникационных узлов из строя.

Ключевые слова: *GERT-модель, компьютерный вирус, информационно-телекоммуникационная система*

Постановка проблемы в общем виде и анализ литературы

В настоящее время в современных информационно-телекоммуникационных системах (ИТС) в процессе их эксплуатации возникает множество нештатных ситуаций, обусловленных нестационарностью входной нагрузки, конечной надежностью и отказоустойчивостью ее элементов, внешними дестабилизирующими воздействиями, требующими автоматических или стационарных управляющих вмешательств в процесс функционирования системы.

Для решения прикладных задач сетевого управления и разработки соответствующих аппаратных или программных средств и приложений остаются актуальными вопросы математического моделирования технологий и процессов сопровождающих информационный обмен (маршрутизации, коммутации, управления и др.). Именно эти вопросы являются одними из наиболее важных и одновременно сложных на этапах проектирования и внедрения ИТС.

Анализ литературы [2 - 12] показал, что в настоящее время существует множество подходов и направлений математического моделирования ИТС и компьютерных сетей. Однако большинство задач, возникающих при управлении, оптимизации, тестировании, оценке вероятностно-временных характеристик, параметров надежности, отказоустойчивости, информационной и функциональной безопасности значительно упрощаются, если их рассматривать на теоретико-графовых моделях.

В работах [4 - 12] проведен анализ и сравнительные исследования основных направлений графового подхода математического моделирования информационно-телекоммуникационных и компьютерных систем и сетей. При этом выявлено, что большинство из указанных выше задач сетевого планирования с минимальной погрешностью можно успешно решить с помощью математического моделирования на основе GERT-сетей.

Разработка графо-аналитических моделей GERT связана с именем американского математика Алана Прицкера [11, 12]. Однако потенциальные возможности математического аппарата GERT-сетей в отдельных направлениях и приложениях современных ИТС в настоящее время полностью не использованы.

Проведенные исследования показали, что существует необходимость в усовершенствовании математических моделей технологии распространения злоумышленного программного обеспечения и антивирусной защиты. Особенно остро эта проблематика выглядит в условиях использования процедур информационного обмена метаданными с облачными антивирусными системами для проведения эвристического и сигнатурного анализа, важного в условиях динамически возрастающих угроз злоумышленного программного обеспечения (ЗПО).

Основная часть

В современных условиях динамичного развития информационно-телекоммуникационных технологий все большую важность приобретают программные средства контроля и управления информационными ресурсами. При этом на практике очень часто возникает проблема несанкционированного проникновения в

программное обеспечение ИТС путем внедрения ЗПО.

Проведенные исследования [2] показали, что в настоящее время существует и постоянно обновляется большое количество подобного рода вредоносных программ, оказывающих значительное влияние на процесс нормального функционирования ИТС. Анализ злоумышленного программного обеспечения позволил представить общую классификацию программных угроз и вредоносного программного обеспечения в виде схемы рис. 1.

Как видно из рис. 1. такие программы можно разделить на две категории:

– требующие программу-носитель;
– независимые программы.

К первой категории относится программный код, который не может работать независимо от некоторой реальной прикладной программы, утилиты или системной утилиты. Ко второй категории принадлежат самостоятельные программы, которые могут быть запущены стандартными средствами операционной системы, как любая другая программа.

Следует заметить, что хотя классификация, приведенная на рис. 1, и позволяет систематизировать информацию о разнородности злоумышленного программного обеспечения, она не дает полного описания реальной картины (например, логические бомбы и "троянские программы" могут быть частями вируса или "червя" и т.д.).

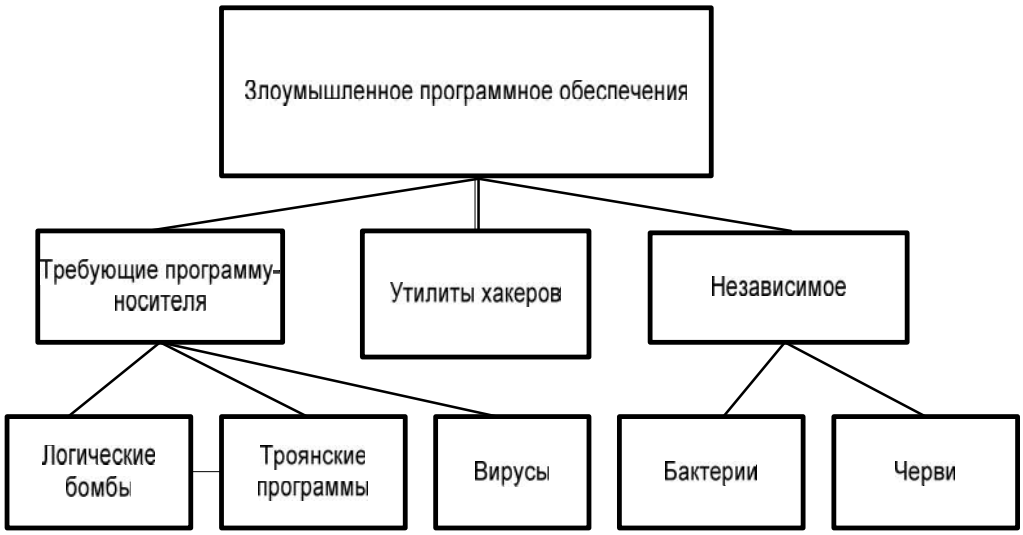

Рис. 1. Классификация злоумышленного программного обеспечения

Анализ литературы [2, 8], а так же проведенные исследования широкого спектра существующих компьютерных вирусов показали, что наиболее опасными в настоящее время представляются вирусы типа Flame. Их отличительной особенностью является наличие множества компонентов кода, функцией которых является выполнение разнообразных вредоносных действий: размножение в сетях различных типов с использованием различных протоколов, похищение и уничтожение конфиденциальной информации, вывод из строя компьютерных систем, шпионаж, взаимодействие с злоумышленным программным обеспечением другого типа и т. д.

Исследования компьютерных вирусов типа Flame позволили выделить основные этапы технологии их распространения в ИТС и проиллюстрировать ее структурно-логическую модель в виде диаграммы переходов, представленной на рис. 2.

Как видно из этого рисунка процесс функционирования оконечного оборудования (узлов) ИТС в условиях распространения исследуемого типа компьютерных вирусов можно представить в виде совокупности состояний:

– телекоммуникационные узлы заражены (I);
– телекоммуникационные узлы не заражены (S);
– телекоммуникационные узлы вылечены и обладают иммунитетом (R);
– зараженные телекоммуникационные узлы с выявленным компьютерным вирусом (D);
– в результате действий злоумышленного программного обеспечения телекоммуникационные узлы полностью вышли из строя (X);

– в результате действий злоумышленного программного обеспечения телекоммуникационные узлы частично вышли из строя (P). Представленная на рис. 2. модель может быть описана следующим образом. Ветвь $S \to I$ (W_{SI}) интерпретирует процесс проникновения компьютерного вируса в незараженный k-й компьютер с вероятностью $P_{зар}^{(k,s^{(i)})}$ в некотором исходном состоянии ИТС $s^{(i)}$.

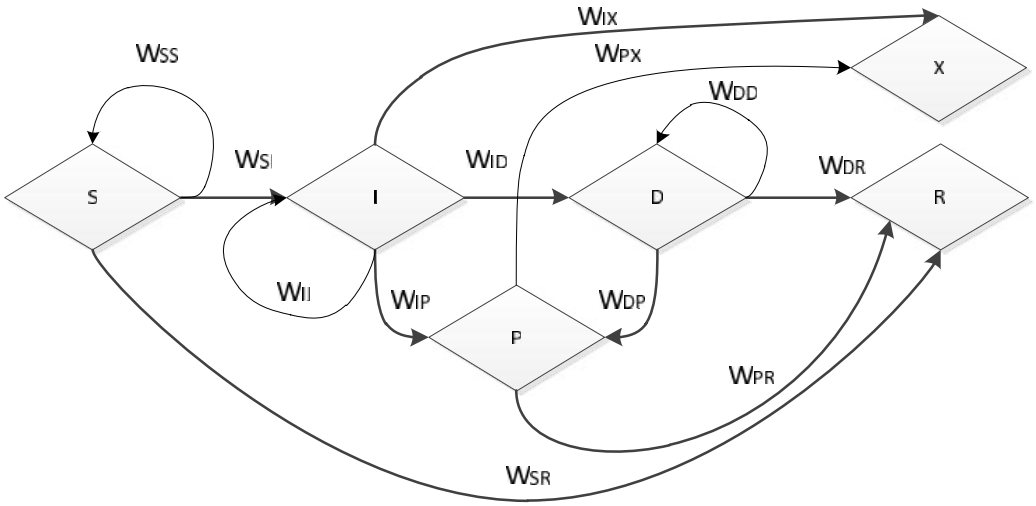

Рис. 2. Структурно-логическая GERT-модель технологии распространения компьютерных вирусов типа Flame

Ветвь $S \to R$ (W_{SR}) описывает процесс иммунизации незараженного k-го компьютера в исходном состоянии с вероятностью иммунизации $P_{им}^{(k,s^{(i)})}$. Ветвь $S \to S$ (W_{SS}) интерпретирует процесс нормального функционирования системы (без заражения) с вероятностью $\left(1 - P_{зар}^{(k,s^{(i)})} - P_{им}^{(k,s^{(i)})}\right)$. Ветвь $I \to D$ (W_{ID}) характеризует процесс детектирования зараженного k-го компьютера в некотором исходном состоянии ИТС $s^{(i)}$ с вероятностью $P_{дет}^{(k,s^{(i)})}$. Ветвь $I \to X$ (W_{IX}) описывает процесс полного выведения из строя k-ого узла с вероятностью $P_{вис}^{(k,s^{(i)})}$. Ветвь $I \to P$ (W_{IP}) интерпретирует процесс частичного выведения k-ого узла из строя с вероятностью $P_{чвис}^{(k,s^{(i)})}$. Ветвь $I \to I$ (W_{II}) предусматривает возможность ситуации, когда узел телекоммуникации останется зараженным с вероятностью $\left(1 - P_{дет}^{(k,s^{(i)})} - P_{вис}^{(k,s^{(i)})} - P_{чвис}^{(k,s^{(i)})}\right)$. Ветвь $D \to R$ (W_{DR}) описывает процесс лечения зараженного k-го компьютера в некотором состоянии ИТС $s^{(i)}$ с вероятностью $P_{леч}^{(k,s^{(i)})}$. Ветвь $D \to P$ характеризует процесс частичного выхода из строя оборудования после того как злоумышленное программное обеспечение типа Flame обнаружено. При этом вероятность такого перехода равна $P_{чв}^{(k,s^{(i)})}$. Ветвь $D \to D$ (W_{DD}) предусматривает возможность ситуации, когда телекоммуникационный узел выявит злоумышленное программное обеспечение типа Flame, но при этом процесса иммунизации не произойдет (обнаружение с помощью только эвристического анализатора). При этом вероятность такого перехода состояния равна $\left(1 - P_{леч}^{(k,s^{(i)})} - P_{чв}^{(k,s^{(i)})}\right)$. Ветвь $P \to R$ (W_{PR}) интерпретирует процесс восстановления нормального работоспособного состояния и иммунизации оборудования после ситуации частичного выхода из строя. Вероятность такого события в некотором состоянии ИТС $s^{(i)}$ равна $P_{лечв}^{(k,s^{(i)})}$. Ветвь $P \to X$ (W_{PX}) описывает процесс полного выхода из строя зараженного телекоммуникационного оборудования с вероятностью $\left(1 - P_{лечв}^{(k,s^{(i)})}\right)$.

Следует заметить, что для упрощения разрабатываемой GERT-модели принято решение не рассматривать остальные переходы в связи с поставленными при моделировании ограничениями («состояние «выведенный из строя» – конечное

состояние объекта», «иммунизированный узел конечная точка модели», «незараженный узел не может быть выведен из строя», «процесс лечения и иммунизации без предварительного детектирования не предусмотрен»), при этом предполагается, что вероятность переходов $R \to R$ и $X \to X$ равна единице, а вероятности оставшихся переходов равны нулю.

Указанные выше допущения и ограничения позволили сформировать матрицу вероятностей переходов из одного состояния в другое и представить ее в виде рис. 3.

$$\begin{array}{c|cccccc}
 & S & I & D & P & R & X \\
S & \left(1 - P_{зар}^{(k,s^{(i)})} - P_{им}^{(k,s^{(i)})}\right) & P_{зар}^{(k,s^{(i)})} & 0 & 0 & P_{им}^{(k,s^{(i)})} & 0 \\
I & 0 & \left(1 - P_{дет}^{(k,s^{(i)})} - P_{вис}^{(k,s^{(i)})} - P_{чвис}^{(k,s^{(i)})}\right) & P_{дет}^{(k,s^{(i)})} & P_{чвис}^{(k,s^{(i)})} & 0 & P_{вис}^{(k,s^{(i)})} \\
D & 0 & 0 & \left(1 - P_{леч}^{(k,s^{(i)})} - P_{чв}^{(k,s^{(i)})}\right) & P_{чв}^{(k,s^{(i)})} & P_{леч}^{(k,s^{(i)})} & 0 \\
P & 0 & 0 & 0 & 0 & P_{лечв}^{(k,s^{(i)})} & \left(1 - P_{лечв}^{(k,s^{(i)})}\right) \\
R & 0 & 0 & 0 & 0 & 1 & 0 \\
X & 0 & 0 & 0 & 0 & 0 & 1
\end{array}$$

Рис. 3. Матрица вероятностей переходов между состояниями в соответствии с GERT-моделью технологии распространения компьютерных вирусов типа Flame

Таблица 1

Характеристики ветвей модели

№ п/п	Ветвь	W-функция	Вероятность	Производящая функция моментов
1.	(S,S)	W_{SS}	1- p_1- p_2	$\lambda_1/(\lambda_1 - s)$
2.	(S,I)	W_{SI}	p_1	$\lambda_2/(\lambda_2 - s)$
3.	(S,R)	W_{SR}	p_2	$\lambda_3/(\lambda_3 - s)$
4.	(I,D)	W_{ID}	p_4	$\lambda_4/(\lambda_4 - s)$
5.	(I,P)	W_{IP}	p_5	$\lambda_5/(\lambda_5 - s)$
6.	(I,X)	W_{IX}	p_6	$\lambda_6/(\lambda_6 - s)$
7.	(I,I)	W_{II}	1- p_4 - p_5- p_6	$\lambda_7/(\lambda_7 - s)$
8.	(D,P)	W_{DP}	p_7	$\lambda_5/(\lambda_5 - s)$
9.	(D,R)	W_{DR}	p_8	$\lambda_8/(\lambda_8 - s)$
10.	(D,D)	W_{DD}	1- p_7 - p_8	$\lambda_9/(\lambda_9 - s)$
11.	(P,R)	W_{PR}	p_9	$\lambda_8/(\lambda_8 - s)$
12.	(P,X)	W_{PX}	1- p_9	$\lambda_6/(\lambda_6 - s)$

Анализ ряда работ [3 - 9], а также проведенные исследования процесса передачи данных в ИТС позволили сформировать характеристики рассмотренных в GERT-модели ветвей и параметры распределения и представить их в табл. 1.

В соответствии с характеристиками ветвей GERT-сети эквивалентную W-функцию времени распространения в ИТС компьютерных вирусов типа Flame с конечным результатом лечения и иммунизации узлов ИТС можно представить формулой (1).

Эквивалентную W-функцию времени распространения в ИТС компьютерных вирусов типа Flame с конечным результатом выхода узлов ИТС из строя можно представить формулой (2).

Следует заметить, что рассматриваемая на рис. 2. GERT-сеть описывает технологию распространения злоумышленного программного

обеспечения на высоком уровне стратификации [11]. В этой связи эквивалентная W-функция времени распространения в ИТС компьютерных вирусов исследуемого типа представляется с одной стороны достаточно сложной для анализа, а с другой стороны в связи с введенными ограничениями моделирования (выбрана однотипная производящая функция моментов, ветви W_{IX}, W_{PX}, так же как и ветви W_{DR}, W_{PR}, а также W_{DP}, W_{IP} характеризуются одним и тем же параметром распределения и др.) точность результатов не отвечает выдвигаемым требованиям.

$$W_E(s) = \frac{W_{SI}W_{ID}W_{DR} + W_{SI}W_{IP}W_{PR} + W_{SI}W_{ID}W_{DP}W_{PR} + W_{SR}}{1 - W_{SS} - W_{SI}W_{II} - W_{SI}W_{ID}W_{DD}} =$$

$$= \frac{p_1(\lambda_2/\lambda_2 - s)(\lambda_8/\lambda_8 - s)\begin{pmatrix} p_4p_8(\lambda_4/\lambda_4 - s) + p_5p_9(\lambda_5/\lambda_5 - s) + \\ + p_4p_7p_9(\lambda_4/\lambda_4 - s)(\lambda_5/\lambda_5 - s) \end{pmatrix}}{1 - (1 - p_1 - p_2)(\lambda_1/\lambda_1 - s) - p_1(\lambda_2/\lambda_2 - s)\times} . \quad (1)$$

$$\times\begin{pmatrix} (1 - p_4 - p_5 - p_6)(\lambda_7/\lambda_7 - s) + \\ + (p_4(1 - p_7 - p_8)(\lambda_4/\lambda_4 - s)(\lambda_9/\lambda_9 - s)) \end{pmatrix}$$

$$W_E(s) = \frac{W_{SI}W_{IX} + W_{SI}W_{IP}W_{PX} + W_{SI}W_{ID}W_{DP}W_{PX}}{1 - W_{SS} - W_{SI}W_{II} - W_{SI}W_{ID}W_{DD}} =$$

$$= \frac{p_1(\lambda_2/\lambda_2 - s)\begin{pmatrix} p_6(\lambda_6/\lambda_6 - s) + \\ + (1 - p_9)(\lambda_5/\lambda_5 - s)(\lambda_6/\lambda_6 - s)(p_5 + p_4(\lambda_4/\lambda_4 - s)) \end{pmatrix}}{1 - (1 - p_1 - p_2)(\lambda_1/\lambda_1 - s) - p_1(\lambda_2/\lambda_2 - s)\times} . \quad (2)$$

$$\times\begin{pmatrix} (1 - p_4 - p_5 - p_6)(\lambda_7/\lambda_7 - s) + \\ + (p_4(1 - p_7 - p_8)(\lambda_4/\lambda_4 - s)(\lambda_9/\lambda_9 - s)) \end{pmatrix}$$

Анализ ряда работ [11, 12] показал, что в этой ситуации для устранения указанных недостатков целесообразно сузить область определения разрабатываемой математической модели путем декомпозиции и эквивалентных упрощающих преобразований.

Проведенные исследования показали, что использование наиболее известного подхода декомпозиции общей задачи математического моделирования на ряд частных задач в большинстве случаев позволяет решить поставленные задачи с заданной точностью. Однако в некоторых случаях простое использование метода декомпозиции не позволяет достичь необходимого уровня вычислительной сложности. Поэтому в диссертационной работе для решения задачи математического моделирования технологии распространения компьютерных вирусов типа Flame с помощью GERT-сетей предлагается комплексное использование подходов декомпозиции и эквивалентных упрощающих преобразований.

Для этого можно воспользоваться методикой, представленной в работах [9, 10]. В соответствии с этой методикой первым шагом математического GERT-моделирования является декомпозиция рассматриваемого объекта на страты и выбор из них наиболее проблемной области исследования.

Проведенные исследования показали, что процесс стратификации GERT-модели выбранной проблемной области является во многом субъективным, и только разработчик, исходя из своего понимания цели моделирования, может определить уровни детализации, число и взаимосвязи элементов. Для процесса функционирования ИТС в ходе выявления, лечения и иммунизации компьютерных вирусов типа Flame рекомендуется определить разбиение на страты.

Анализ процессов протекающих в ИТС показал, что в условиях внешних деструктивных воздействий компьютерных вирусов типа Flame одними из основных этапов, позволяющих достичь состояния R (см. рис. 1) (телекоммуникационные узлы вылечены и обладают иммунитетом) являются этапы выявления, лечения и иммунизации злоумышленного программного обеспечения.

Особенно важным данный уровень стратификации представляется при математическом описании процессов выявления, лечения и иммунизации с помощью «облачных» антивирусных систем, поскольку именно на этом уровне возможен учет основных протоколов передачи данных транспортного (TCP, UDP) и сетевого (OSPF, RIP, BGP и др.) уровней.

Процедура эквивалентного упрощающего преобразования GERT-сети к эквивалентной дуге представляется набором элементарных операций преобразования, в результате которых можно получить эквивалентные характеристические

функции [9]. Общая методика эквивалентного упрощающего преобразования GERT-сети а также основные математические выкладки, характеризующие данную методику представлены в работах [9, 10].

Выводы

Таким образом, разработана структурно-логическая GERT-модель технологии распространения компьютерных вирусов, что в итоге позволило представить эквивалентную W-функцию времени распространения в ИТС наиболее опасных компьютерных вирусов типа Flame с конечными результатами лечения и иммунизации узлов ИТС, а также выхода телекоммуникационных узлов из строя.

Список литературы

1. Анго А. Математика для электро- и радиоинженеров / А. Анго.– М.:Наука, 1964. – 772 с.

2. Кузнецов О.О. Протоколи захисту інформації у комп'ютерних системах та мережах / О.О. Кузнецов, С.Г. Семенов. – Х.: ХНУРЕ, 2009. – 184 с

3. Майника Э. Алгоритмы оптимизации на сетях и графах: пер. с англ. / Э. Майника; под ред. Е.К. Масловского. – М.: Мир, 1981. – 321 с.

4. Семенов С.Г. Математическая модель мультисервисного канала связи на основе экспоненциальной GERT-сети / С.Г.Семенов, Е.В.Мелешко, Илюшко Я.В. // Науковий журнал «Системи озброєння і військова техніка»., - Х.:ХУ ПС, - 2011.-Вип. 3(27) .- С.64-67.

5. Семенов С.Г. Исследования вероятностно-временных характеристик мультисервисного канала связи с использованием математического аппарата GERT-сети / С.Г. Семенов, В.В. Босько, І.А. Березюк // Системи обробки інформації. – Х.: ХУ ПС. – 2012. – Том 1. Вип. 3(101). – С. 139-142.

6. Семенов С.Г. Моделирование защищенного канала связи с использованием экспоненциальной GERT-сети / С.Г. Семенов, А.А. Можаев // Информатика, математическое моделирование, экономика. – Смоленськ.: Смоленский филиал АНО ВПО ЦС РФ "Российский университет кооперации". – 2012. – Том.1. – С. 152-160.

7. Семенов С.Г. Математическая модель процесса доставки информационных пакетов в компьютерной сети системы критического применения / С.Г.Семенов, И.В. Ильина. // Науково-технічний журнал «Радіоелектронні і комп'ютерні системи», – Х.:ХАІ, 2008. Вип. 1(28) С.162-165.

8. Семенов С.Г. Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом / С.Г. Семенов, В.В. Давыдов // Вісник Національного технічного університету «ХПІ». – Х.:НТУ «ХПІ». – 2012. –№38. – С 163-171

9. Семенов С.Г. Методика математического моделирования защищенной ИТС на основе многослойной GERT-сети / С.Г. Семенов // Вісник Національного технічного університету «Харківський політехнічний інститут». – Х.:НТУ «ХПІ». – 2012. –№62 (968). – С 173-181.

10. Шибанов А.П. Нахождение закона распределения выходной величины GERT-сети большой размерности / А.П. Шибанов // Информационные технологии, 2002. № 1. С. 42 45.

11. Pritsker A. A. B. Modeling and analysis using Q-GERT networks New York : Wiley : Distributed by Halsted Press, 1979.

12. Pritsker A. A. B., Happ W. W. GERT: Graphical Evaluation and ReviewTechnique. Part I. Fundamentals // The Journal of Industrial Engineering (May 1966).

Поступила в редакцію 27.01.2014

Рецензент: д-р техн. наук, с.н.с. Е.С. Козелкова, Государственный университет телекоммуникаций, Киев.

СТРУКТУРНО-ЛОГІЧНА GERT-МОДЕЛЬ ТЕХНОЛОГІЇ РОЗПОВСЮДЖЕННЯ КОМП'ЮТЕРНИХ ВІРУСІВ

О.А. Смірнов, І.А. Березюк, Мохамад Абу Таам Ганн

Розроблена структурно-логічна GERT-модель технології поширення комп'ютерних вірусів, що дозволила отримати аналітичний вираз для розрахунку еквівалентної W-функції часу поширення в інформаційно-телекомунікаційних системах найбільш небезпечних комп'ютерних вірусів типу Flame з кінцевими результатами лікування та імунізації вузлів інформаційно-телекомунікаційних систем, а також виходу телекомунікаційних вузлів з ладу.

Ключові слова: *GERT-модель, комп'ютерний вірус, інформаційно-телекомунікаційна система.*

STRUCTURAL LOGIC GERT- MODEL TECHNOLOGY SPREAD OF COMPUTER VIRUSES

A.A. Smirnov, I.A. Berezyuk, Mohamad Abou Taam

Developed structural logic GERT- technology model the spread of computer viruses, which allowed to obtain an analytical expression for calculating the equivalent W- function of time dissemination of information and telecommunication systems, the most dangerous type of computer viruses Flame with the end results of treatment and immunization sites information and telecommunication systems , as well as output telecommunication nodes fail.

Keywords*: GERT-model, a computer virus, information-telecommunications system.*