Захист інформації

УДК 004.7

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

Кировоградский национальный технический университет, Кировоград

МАТЕМАТИЧЕСКАЯ GERT-МОДЕЛЬ ТЕХНОЛОГИИ ПЕРЕДАЧИ МЕТАДАННЫХ В ОБЛАЧНЫЕ АНТИВИРУСНЫЕ СИСТЕМЫ

Проведен анализ подходов и возможностей математического моделирования современных телекоммуникационных сетей с помощью GERT-систем. Исследована структура процесса передачи метаданных в облачные антивирусные системы. Разработана математическая модель технологии передачи метаданных в облачные антивирусные системы на основе GERT-сети. Получено аналитическое выражение для расчета плотности распределения времени передачи метаданных в сети с учетом показатели реальной надежности и особенности многопутевой маршрутизации.

Ключевые слова: *облачные антивирусные системы, злоумышленное программное обеспечение, математическая модель, граф, GERT-сети.*

Введение

Постановка проблемы. 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 не использованы полностью.

Одним из таких направлений, является процесс информационного обмена метаданными с облачными антивирусными системами для проведения эвристического и сигнатурного анализа, особенно важного в условиях динамически возрастающих угроз злоумышленного программного обеспечения (ЗПО).

Целью статьи является разработка математической модели технологии передачи данных в процессе информационного обмена специализированными сигнатурами с облачными антивирусными системами на основе GERT-сети. При этом должны быть учтены показатели реальной надежности и особенности многопутевой маршрутизации.

Основная часть.

В последнее время у пользователей ИТС все большим спросом пользуются услуги облачных антивирусных систем. Связано это во многом с одной стороны с динамическим развитием сетевых технологий, а с другой, ростом реальных угроз ЗПО, справиться с которым стационарные антивирусные системы не в состоянии [9].

Процесс информационного обмена оконечных рабочих станций с узлами, предоставляющими услуги облачной антивирусной защиты, представляет собой четко организованную функциональную структуру, являющуюся совокупностью алгоритмов формирования сигнатур, транспортировки, коммутации, маршрутизации и обработки специализированными анализаторами.

Обобщенная структура и временная диаграмма процесса передачи метаданных в облачные антивирусные системы для выявления ЗПО представлена на рис. 1.

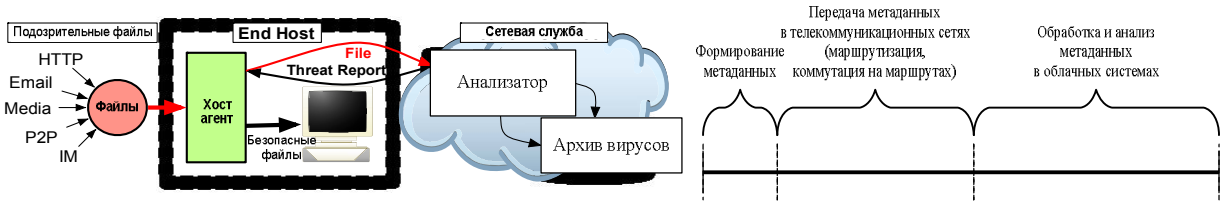

Рис. 1. Обобщенная структура и временная диаграмма процесса передачи метаданных в облачные антивирусные системы

Проведенные исследования основных подходов математического моделирования показали, что наиболее удобной, наглядной и многосторонней формой описания технологии передачи метаданных в облачные антивирусные системы является граф алгоритмов на основе GERT-сети.

Для рассматриваемого в статье примера под графом алгоритмов понимается орграф G = (X, U) вершины x_i которого отображают частные реализации i-х алгоритмов системы. Вершинам графа приписывается вес, соответствующий времени реализации алгоритма. (В отдельных случаях это может быть вероятность показания на тот или иной выход узлов графа, требующаяся для выполнения память, ошибки определения тех или иных величин, связанных с реализацией алгоритма и т.д.). Частные реализации алгоритмов в рассматриваемом графе GERT-сети отождествляется дугами графа с определенными условными вероятностями и производящими функциями моментов ветви.

Воспользуемся представленными на рис. 1 данными для разработки GERT-модели ИТС в процессе передачи метаданных в облачные антивирусные системы. Типовая модель алгоритмов формирования и передачи метаданных в облачные антивирусные системы представлена на рис. 2.

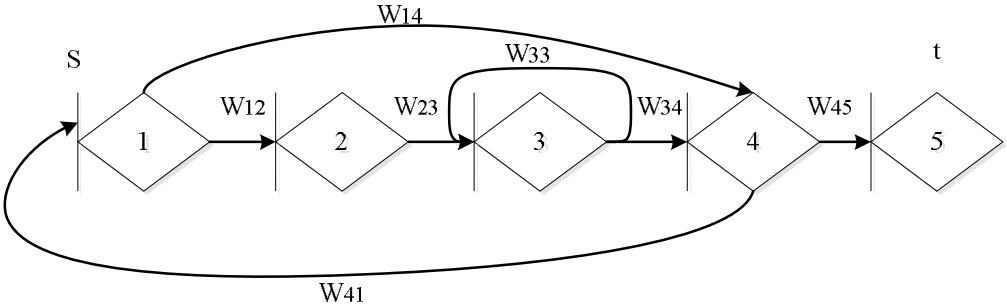

Рис. 2. Модель алгоритмов формирования и передачи метаданных в облачные антивирусные системы

Эта модель может быть описана следующим образом. Ветвь (1,2) интерпретирует время формирования метаданных (сигнатур). Ветвь (2,3) задает время передачи кадра (пакета) метаданных от передатчика к трансляторам (маршрутизаторам). Ветвь (3,3) отображает возможное неисправное состояние транслирующего коммутационного оборудования (маршрутизаторов) на выбранных маршрутах. Ветвь (3,4) описывает время коммутации кадра(пакета) в телекоммуникационном оборудовании. Ветви (4,1) и (4,5) задают случайное время передачи квитанции о правильности (ошибке) доставки кадров (пакетов) в соответствии с протоколом транспортного уровня (TCP).

Узел 5 отражает состояние системы в момент анализа метаданных на предмет наличия ЗПО.

В ряде практических случаев с целью повышения вероятности выявления ЗПО существует необходимость антивирусного анализа не сформированных на оконечном оборудовании сигнатур, а данных, хранимых на этом оборудовании в полном объеме. Этой ситуации соответствует ветвь (1,4).

Ветви (3,4), (4,1) и (4,5) целесообразно описывать идентичными параметрами распределения, так как они задают схожие операции передачи данных небольшого объема.

Анализ ряда работ [5,7,8], а также проведенные исследования процесса передачи данных в мультисервисных телекоммуникационных сетях позволили сформировать характеристики ветвей и параметры распределения в виде, представленном в табл. 1.

Таблица 1

Характеристики ветвей модели

№ п/п	Ветвь	W-функция	Вероятность	Производящая функция моментов
1	(1,2)	W_{12}	p_1	$\lambda_1 / (\lambda_1 - s)$
2	(1,4)	W_{14}	$1\text{-}p_1$	$\lambda_2 / (\lambda_2 - s)$
3	(2,3)	W_{23}	p_2	$\lambda_3 / (\lambda_3 - s)$
4	(3,3)	W_{33}	p_3	$\lambda_4 / (\lambda_4 - s)$
5	(3,4)	W_{34}	1- p3	$\lambda_5 / (\lambda_5 - s)$
6	(4,5)	W_{45}	p_4	$\lambda_5 / (\lambda_5 - s)$
7	(4,1)	W_{41}	$1\text{-}\ p_4$	$\lambda_5 / (\lambda_5 - s)$

Анализ данных, представленных в табл. 1 показал высокую структурную сложность разрабатываемой GERT-сети. Особенно остро данная проблема фиксируется на участке, сформированном из узлов 2-3-4 (ветви (2,3), (3,3)).

С целью упрощения рассматриваемой на рис. 2 модели воспользуемся методикой эквивалентных упрощающих преобразований, описанной в работах [7, 10].

В результате упрощающих преобразований сформируем GERT-сеть, представленную на рис. 3. Как видно из этого рисунка в результате упрощающих преобразований ветви (2,3) и (3,3) были заменены на эквивалентную ветвь. Обновленные данные характеристик ветвей сети представлены в табл. 2.

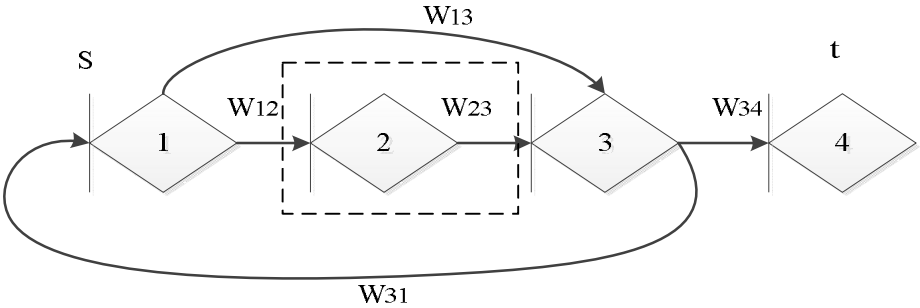

Рис. 3. Упрощенная модель алгоритмов формирования и передачи метаданных в облачные антивирусные системы

Таблица 2

Характеристики ветвей модели

№	Ветвь	W-фун-я	Параметр распределения
1	(1,2)	W_{12}	$p_1\lambda_1 / (\lambda_1 - s)$
2	(1,3)	W_{13}	$(1\text{-}p_1)\ \lambda_2 / (\lambda_2 - s)$
3	(2,3)	W_{23}	$\dfrac{p_2\lambda_3}{(\lambda_3 - s)((\lambda_4 - s) - p_3\lambda_4)}$
4	(3,4)	W_{34}	$p_4\lambda_5 / (\lambda_5 - s)$
5	(3,1)	W_{31}	$(1 - p_4)\lambda_5 / (\lambda_5 - s)$

В соответствии с характеристиками ветвей GERT-сети определим эквивалентную W-функцию времени передачи файла как

$$W_E(s) = \frac{W_{13}W_{34} + W_{12}W_{23}W_{34}}{1 - W_{13}W_{31} - W_{12}W_{23}W_{31}} =$$

$$= \frac{\dfrac{\left(\begin{array}{c} p_4\lambda_5 q_1\lambda_1(\lambda_1 - s)(\lambda_3 - s)((\lambda_4 - s) - p_3\lambda_4) + \\ p_1\lambda_1 p_4\lambda_5 p_2\lambda_3(\lambda_2 - s) \end{array}\right)}{(\lambda_2 - s)(\lambda_5 - s)(\lambda_3 - s)((\lambda_4 - s) - p_3\lambda_4)}}{\dfrac{\left(\begin{array}{c} (\lambda_1 - s)(\lambda_2 - s)(\lambda_5 - s)(\lambda_3 - s)\times \\ \times((\lambda_4 - s) - p_3\lambda_4) - q_1\lambda_2 q_4\lambda_5 \times \\ \times(\lambda_1 - s)(\lambda_3 - s)((\lambda_4 - s) - p_3\lambda_4) - \\ -p_1\lambda_1 q_4\lambda_5 p_2\lambda_3(\lambda_2 - s) \end{array}\right)}{(\lambda_2 - s)(\lambda_1 - s)(\lambda_5 - s)(\lambda_3 - s)((\lambda_4 - s) - p_3\lambda_4)}},$$

где $1 - p_1 = q_1$, $1 - p_2 = q_2$, $1 - p_3 = q_3$, $1 - p_4 = q_4$.

Проведенные исследования показали, что в сложных GERT-сетях с возможными циклами отсутствуют простые методы нахождения особых точек функции $\Phi_{\text{Ä}}(z)$ замены действительных переменных $(z = -i\varsigma)$, где ς – действительная переменная. Связано это с тем, что для нахождения особых точек необходимо решать нелинейные уравнения, и чем сложнее структура GERT-сети, тем сложнее и исходное уравнение [1 – 5]. Поэтому в ходе моделирования выполняя комплексное преобразование получим:

$$\Phi(z) = \frac{uz^3 - kz^2 + wz + h}{\left(z^3 + vz^2 + rz + c\right)}, \qquad (1)$$

где $u = p_4\lambda_5 q_1\lambda_2$,

$$k = p_4\lambda_4 q_1\lambda_2(p_3\lambda_4 - \lambda_3 - \lambda_1 - \lambda_4),$$

$$w = p_4\lambda_5 q_1\lambda_2 \times$$

$$\times(p_3\lambda_3\lambda_4 - \lambda_1\lambda_3 - \lambda_3\lambda_4 - \lambda_1\lambda_4 + p_3\lambda_1\lambda_4);$$

$$h = p_4\lambda_4 q_1\lambda_1\lambda_2\lambda_3\lambda_4 q_3,$$

$$v = \lambda_3 - \lambda_4 - \lambda_2 + q_1 q_4\lambda_2\lambda_5 + p_3\lambda_4,$$

$$r = \lambda_3\lambda_4 + \lambda_3\lambda_2 - q_1\lambda_2 q_4\lambda_5\lambda_3 - p_3\lambda_3\lambda_4 + \lambda_2\lambda_4 -$$

$$-q_1\lambda_2 q_4\lambda_5\lambda_4 - p_3\lambda_2\lambda_4 + q_1\lambda_2 q_4\lambda_5 p_3\lambda_4;$$

$$c = \lambda_3\lambda_4\lambda_2 - q_1\lambda_2 q_4\lambda_3\lambda_4\lambda_5 - p_3\lambda_3\lambda_4\lambda_2 + \\ + q_1\lambda_2 q_4\lambda_3\lambda_4 p_3.$$

Из выражения (1) видно, что функция $\Phi(z)$ имеет только простые полюсы определяемые корнями уравнения $z^3 + vz^2 + rz + c = 0$. В этом случае плотность распределения вероятностей времени передачи сообщения равна:

$$\phi(x) = \frac{1}{2\pi i}\int_{-i\infty}^{i\infty} e^{zx}\frac{uz^3 - kz^2 + wz + h}{\left(z^3 + vz^2 + rz + c\right)}dz. \quad (2)$$

Используя специализированный математический пакет Mathcad определим простые полюсы z функции $\Phi(z)$ и найдем плотность распределения вероятностей $\phi(x)$ времени передачи метаданных в «облачные» антивирусные системы.

При этом в качестве начальных данных определим следующие параметры ветвей GERT-сети:

$$p_1 = 0{,}9,\ p_2 = 0{,}99999,$$
$$p_3 = 0{,}99999,\ p_4 = 0{,}99999,$$
$$\lambda_1 = 1,\ \lambda_2 = 0{,}099,$$
$$\lambda_3 = 0{,}9,\ \lambda_4 = 0{,}5,\ \lambda_5 = 0{,}4.$$

Для указанного примера функция $\Phi(z)$ имеет простые полюса:

$$z := \begin{pmatrix} -0.67 \\ 0 \\ -0.117 \end{pmatrix}.$$

В соответствии с формулой (2) $\phi(x)$ рассчитывается так, как приведено на рис. 4.

На рис. 5 представлен график плотности распределения времени передачи мета данных.

Как видно из рис. 5, максимальные значения плотности распределения времени формирования и передачи приходится на промежуток от 1 до 3 с.

$$\frac{1}{z}\,0.159155 \times 2.71828^{(-0.0835025-0.364433\,i)\,z} \\ \Big(z\,2.71828^{(0.920508+0.364433\,i)\,z}\,\mathrm{Ei}((x-0.837005)\,z) \\ (1.02026\,h - 0.714769\,k + 0.85396\,v + 0.598265) + \\ 2.71828^{(0.728866\,i)\,z}\,z\,\mathrm{Ei}((x+(0.0835025-0.364433\,i))\,z) \\ (-(0.142616 - 0.131097\,i)\,k - (0.42698 + 0.293502\,i)\,v + \\ (0.0358675 + 0.0629208\,i) + (-0.510128 + 1.28851\,i)\,h) - \\ (0.510128 + 1.28851\,i)\,h\,z\,\mathrm{Ei}((x+(0.0835025+0.364433\,i))\,z) - \\ (0.142616 + 0.131097\,i)\,k\,z\,\mathrm{Ei}((x+(0.0835025+0.364433\,i))\,z) - \\ (0.42698 - 0.293502\,i)\,v\,z\,\mathrm{Ei}((x+(0.0835025+0.364433\,i))\,z) + \\ (0.0358675 - 0.0629208\,i)\,z\,\mathrm{Ei}((x+(0.0835025+0.364433\,i))\,z) + \\ 2.71828^{z\,(x+(0.0835025+0.364433\,i))}\Big) + \mathrm{constant}$$

Рис. 4. Расчет $\phi(x)$

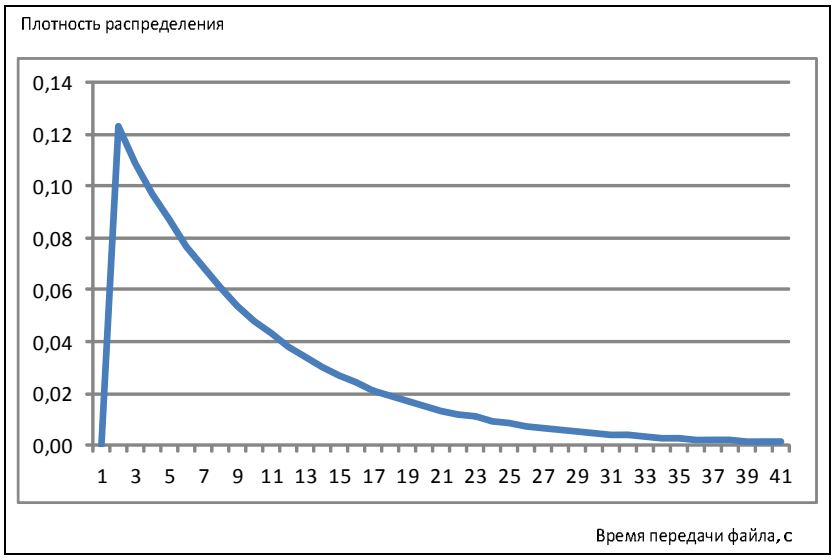

Рис. 5. Плотность распределения времени передачи метаданных в облачные антивирусные системы

Выводы

Таким образом, на основе GERT-сети разработана математическая модель технологии передачи метаданных в облачные антивирусные системы, которая отличается от известных учетом показателей реальной надежности и особенностей многопутевой маршрутизации в соответствии с протоколами сетевого уровня.

Модель может быть использована для исследования процессов и технологий распространения и лечения ЗПО в информационно-телекоммуникационных системах, а также локальных компьютерных сетях, при разработке новых протоколов, алгоритмов и программ управления сетевыми и канальными ресурсами ИТС, проектировании новых средств антивирусной защиты данных.

Применение GERT-сетей в ходе математического моделирования даст возможность использования результатов, полученных в аналитическом виде (функции, плотности распределения) для проведения сравнительного анализа и исследований более сложных информационно-телекоммуникационных систем математическими методами.

Список литературы

1. *Анго А. Математика для электро- и радиоинженеров / А. Анго. – М.: Наука, 1964. – 772 с.*
2. *Вишневский В.М. Теоретические основы проектирования компьютерных сетей / В.М. Вишневский. – М.: Техносфера, 2003. – 512 с.*
3. *Курош А.Г. Курс высшей алгебры / А.Г.Курош. – М.:Наука, 1968. – 431 с.*
4. *Майника Э. Алгоритмы оптимизации на сетях и графах: пер. с англ. / Э. Майника; под ред. Е.К. Масловского. – М.: Мир, 1981. – 321 с.*
5. *Семенов С.Г. Математическая модель мультисервисного канала связи на основе экспоненциальной GERT-сети / С.Г.Семенов, Е.В. Мелешко, Я.В. Илюшко // Науковий журнал «Системи озброєння і військова техніка»., - Х.:ХУ ПС, - 2011.-Вип. 3(27) .- С.64-67.*
6. *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.*
7. *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.*
8. *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.*
9. *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*
10. *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.*
11. *Pritsker A. A. B. Modeling and analysis using Q-GERT networks / A.A.B. Pritsker. – New York : Wiley : Distributed by Halsted Press, 1979.*
12. *Pritsker A.A.B. GERT: Graphical Evaluation and ReviewTechnique. Part I. Fundamentals / A.A.B. Pritsker, W.W. Happ // The Journal of Industrial Engineering (May 1966).*

Поступила в редколлегию 16.12.2013

Рецензент: д-р техн. наук, с.н.с. Г.А. Кучук, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МАТЕМАТИЧНА GERT-МОДЕЛЬ ТЕХНОЛОГІЇ ПЕРЕДАЧІ МЕТАДАНИХ В ХМАРНІ АНТИВІРУСНІ СИСТЕМИ

В.В. Босько, О.А. Смірнов, І.А. Березюк, Мохамад Абу Таам Гані

Проведений аналіз підходів і можливостей математичного моделювання сучасних телекомунікаційних мереж за допомогою GERT-систем. Досліджена структура процесу передачі метаданих в хмарні антивірусні системи. Розроблена математична модель технології передачі метаданих в хмарні антивірусні системи на основі GERT-сети. Отриманий аналітичний вираз для розрахунку щільності розподілу часу передачі метаданих в мережі з обліком показники реальної надійності і особливості багатошляхової маршрутизації.

Ключові слова: *хмарні антивірусні системи, зловмисне програмне забезпечення, математична модель, граф, GERT-мережі.*

MATHEMATICAL GERT- MODEL OF METADATA'S TRANSMISSION TECHNOLOGY IN ANTI-VIRUS SYSTEMS

.B. Bos'ko, A.A. Smirnov, I.A. Berezyuk, Mokhamad Aba of Taam Gani

The analysis of approaches and possibilities of mathematical design of modern telecommunication networks is conducted by the GERT-систем. The structure of process of transmission of metadatas is investigational in anti-virus systems. The mathematical model of technology of transmission of metadatas is developed in anti-virus nephystems on the basis of GERT-сети. Analytical expression is got for the calculation of closeness of distributing of time of transmission of metadatas in a network recognition real reliability and feature of the multiground routing indexes.

Keywords: *anti-virus nephystems, ill-intentioned software, mathematical model, count, GERT-nets.*