

С.Г. СЕМЕНОВ, канд. техн. наук, доц., НТУ "ХПИ", Харьков

МЕТОДИКА МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ЗАЩИЩЕННОЙ ИТС НА ОСНОВЕ МНОГОСЛОЙНОЙ GERT-СЕТИ

На основе теоретико-графового подхода моделирования разработана методика математического моделирования защищенной информационно-телекоммуникационной системы (ИТС), в виде многослойной GERT-сети. Определены наиболее сложные с вычислительной точки зрения этапы моделирования. Разработан алгоритм эквивалентных, упрощающих преобразований GERT-сети. Библиогр.: 8 назв.

Ключевые слова: математическая модель, GERT-сеть, защищенная ИТС.

Постановка проблемы. В настоящее время существует множество средств защиты информации, функционирующих на разных уровнях модели сетей будущего поколения NGN-сетей (Next Generation Network), при этом большинство из этих средств доступны для использования. Одной из основных особенностей существующих средств защиты информации является комплексность в подходах обеспечения основных услуг безопасности, которая возможна объединением различных протоколов, механизмов и алгоритмов в рамках конечного аппаратного или программного изделия. В таких условиях возникает необходимость согласования возможных режимов и параметров функционирования средств защиты информации на разных уровнях NGN-сети между собой.

Анализ литературы [1 – 8] показал, что многие задачи, возникающие при проектировании, тестировании, оптимизации и оценке вероятностно-временных характеристик, а также параметров защищенных ИТС значительно упрощаются, если их рассматривать на теоретико-графовых моделях. Однако задача нахождения закона распределения для моделей большой размерности в данном подходе решается с большой погрешностью (до 20%), что недопустимо в ряде задач, связанных с проектированием систем защиты информации в ИТС. В работах [4 – 6] авторы связывают решение указанной проблемы с разработкой и построением математических моделей в виде GERT-сетей, при этом приведенные результаты моделирования говорят о повышении точности получаемых результатов до 10 – 15%. Однако, анализ существующих методов и методик построения GERT-сетей показал полное отсутствие в этом направлении работ, использующих подход многослойного моделирования.

Поэтому **целью статьи** является разработка и использование методики математического моделирования защищенной ИТС на основе многослойной GERT-сети.

Основные этапы математического моделирования с помощью многослойной GERT-сети. Как показали результаты проведенных исследований [4 – 6], математическое моделирование многоуровневой защищенной ИТС с помощью многослойной GERT-сети может быть осуществлено при выполнении следующих условий:

- для обеспечения услуг безопасности используется несколько средств защиты информации на разных уровнях NGN-архитектуры в комплексе;

- процесс функционирования средств защиты информации на каждом из уровней NGN-архитектуры может быть описан с помощью однослойной GERT-сети;

- процесс функционирования защищенной ИТС в целом представляется в виде последовательных переходов из одного состояния в другое: $S_1^{(\ell)}, S_2^{(\ell)}, \dots$, где $\ell = \{1, 2, 3\}$ – номер уровня NGN-архитектуры;

- каждому из переходов приписывается вероятность $p_k^{(\ell)}$, где k – номер перехода на одном из уровней;

- результирующие вероятности прохождения последовательности состояний на одном уровне в многослойной GERT-сети определяются по правилу умножения $P\left\{S_{k_0}^{(\ell)}, \dots, S_{k_n}^{(\ell)}\right\} = p_{k_0}^{(\ell)} \times \dots \times p_{k_n}^{(\ell)}$;

- результирующие вероятности прохождения последовательности состояний между уровнями многослойной GERT-сети определяется аналогично предыдущему правилу $P\left\{S_{k_0}^{(\ell_j)}, \dots, S_{k_n}^{(\ell_m)}\right\} = p_{k_0}^{(\ell_j)} \times \dots \times p_{k_n}^{(\ell_m)}$;

- $\forall(S_k^{(\ell_j)}, S_k^{(\ell_m)})$ и $(S_{k_j}^{(\ell)}, S_{k_m}^{(\ell)})$ соответствуют условные вероятности $p_k^{(\ell_j, m)}$ и $p_{k_j, m}^{(\ell)}$ соответственно.

Анализ и проведенные исследования процесса функционирования информационно-телекоммуникационных систем позволили определить, что основными этапами математического моделирования защищенной ИТС на основе многослойной GERT-сети являются следующие.

1. Определение уровня детализации (стратификация) и структуризация математической модели защищенной ИТС.

2. Представление защищенной ИТС в виде пространства многослойной GERT-структуры $\bar{G} = (G, C)$, где $G = (\tilde{N}, \tilde{A})$ – подпространство уровней моделирования, $C = (N, A)$ – подпространство стохастических сетей, \tilde{N}, N – GERT-узлы (вершины), \tilde{A}, A – ветви (дуги) GERT-сети.

3. Определение условной вероятности и производящей функции моментов каждой ветви.

4. Вычисление \tilde{W} и W -функций каждой ветви в подпространствах G и C соответственно.

5. Эквивалентные, упрощающие преобразования многослойной GERT-сети.

6. Переход от \tilde{W} и W -функций многослойной GERT-сети к характеристическим функциям $\chi(\zeta)$ и вычисление действительных $\chi_{\text{Re}}(\zeta)$ и мнимых $\chi_{\text{Im}}(\zeta)$ значений характеристических функций дуг в узлах интерполяции.

7. Описание процесса передачи от истока к выходному узлу многослойной GERT-сети на основе топологического уравнения Мейсона.

8. Преобразование многослойной GERT-сети по формуле Мейсона в эквивалентную сеть, состоящую из одной ветви, характеризующейся эквивалентной W -функцией $W_E(s) = p_E M_E(s)$, где p_E – вероятность прохождения стока, $M_E(s)$ – эквивалентная производящая функция моментов.

9. Вычисление действительных $\tilde{X}_{\text{Re}}(\zeta)$ и мнимых $\tilde{X}_{\text{Im}}(\zeta)$ значений эквивалентной характеристической функции $\tilde{X}_E(\zeta) = X_E(\zeta)e^{-0.5\zeta^2}$ GERT-сети в узлах интерполяции.

10. Определение закона распределения и плотности распределения вероятностей искомой случайной величины.

11. Нахождение математического ожидания и дисперсии времени прохождения GERT-сети.

Рассмотрим более подробно каждый из перечисленных этапов математического моделирования.

Стратификация математической модели защищенной ИТС является субъективным процессом, и только разработчик, исходя из своего понимания цели моделирования, может определить уровни детализации, число и взаимосвязи элементов. Для защищенных ИТС рекомендуется определить следующее разбиение на страты.

1) K -страта. Низкоуровневые алгоритмы обработки данных и защиты информации.

2) $(K + 1)$ -страта. Механизмы обеспечения требуемых услуг безопасности.

3) $(K + 2)$ -страта. Низкоуровневое моделирование каналов связи путем задания их типов и параметров, необходимых для выполнения поставленной задачи.

4) $(K + 3)$ -страта. Моделирование каналов связи среднего уровня (с учетом специфики разбиения данных на информационные пакеты и кадры).

5) $(K + 4)$ -страта. Моделирование протоколов и средств защиты информации, коммуникационных протоколов транспортного уровня, протоколов маршрутизации уровня доступа, протоколов, выполняющих транспортные функции и функции доставки сообщений между конечными узлами.

6) $(K + 5)$ -страта. Моделирование приложений с помощью команд нескольких типов, в том числе команд обработки данных, отправки и чтения сообщений, чтения и записи данных в файл, установления сессий и приостановки программы до получения сообщений.

7) $(K + 6)$ -страта. Моделирование информационного трафика различных сетевых служб с учетом характерных особенностей, основных показателей и законов распределения искомым случайных величин.

8) $(K + 7)$ -страта. Моделирование сетей на верхнем уровне абстракции.

После того как разработчик определился с уровнем детализации математической модели защищенной ИТС можно приступать ко второму этапу математического моделирования, представлению защищенной ИТС в виде пространства многослойной GERT-структуры.

На третьем этапе моделирования, при определении условных вероятностей и производящих функций моментов ветвей многослойной GERT-сети, следует учитывать многообразие распределений, которыми могут характеризоваться отдельные дуги (пуассоновское, экспоненциальное, фрактальные распределения и др.). Например, как указано в ряде источников [1, 4 – 6] случайная величина времени доставки информационных пакетов в канале связи может быть распределена по экспоненциальному закону, а тот же самый показатель, но уже характеризующий поведение мультисервисного информационного трафика на маршруте имеет фрактальные свойства. Кроме того, как показали исследования, при математическом моделировании сложных технических систем нельзя пренебрегать возможностью использования непрерывных распределений произвольного вида. Подобного рода данные, чаще всего, определяются эмпирическим путем [4, 5]. Особенно актуальной эта задача представляется на этапе определения производящей функции моментов ветвей, соединяющих различные уровни NGN-архитектура, когда заранее сложно точно выбрать закон распределения вероятности случайной величины.

Следует заметить, что от точности определения условной вероятности и производящей функции моментов зависит результат следующего этапа математического моделирования – вычисления \tilde{W} и W -функций каждой ветви многослойной GERT-сети. На данном этапе \tilde{W} и W -функции вычисляются с помощью выражения:

$$W_{i,j}(\tilde{W}_{i,j}) = p_{i,j} M_X(s), \quad (1)$$

где $p_{i,j}$ – условная вероятность перехода i, j ; $M_X(s)$ – производящая функция моментов ветви i, j .

Операции и процедуры, выполняемые на пятом и шестом этапах моделирования, требуют большего внимания и более подробно будут описаны. А на седьмом этапе математического моделирования на основе многослойной GERT-сети, как показали исследования, удобным и эффективным способом описания процесса передачи от истока к выходному (внутреннему) узлу, является топологическое представление Мейсона [6]:

$$1 - \sum T(L_1) + \dots + (-1)^n \sum T(L_n) = 0, \quad (2)$$

где $\sum T_i$ – суммы эквивалентных коэффициентов пропуска для всех возможных петель i -го порядка.

Уравнение (2) выражает связь эквивалентной W -функции $W_E(s)$ с эквивалентными W -функциями петель первого и i -го порядков.

На восьмом этапе моделирования осуществляется вычисление эквивалентной $W_E(s)$ функции по формуле:

$$W_E(s) = \frac{\sum_{\gamma_1=1}^{r_1} \prod_{\sigma_1=1}^{\Delta_1} \hat{W}_{\gamma_1 \sigma_1}^1 + \dots - (-1)^m \sum_{\gamma_m=1}^{r_m} \prod_{\sigma_m=1}^{\Delta_m} \hat{W}_{\gamma_m \sigma_m}^m}{1 - \sum_{\alpha_1=1}^{A_1} \prod_{\beta_1=1}^{B_1} \bar{W}_{\alpha_1 \beta_1}^1 + \dots + (-1)^\ell \sum_{\alpha_\ell=1}^{A_\ell} \prod_{\beta_\ell=1}^{B_\ell} \bar{W}_{\alpha_\ell \beta_\ell}^\ell}, \quad (3)$$

где $\prod_{\sigma_i=1}^{\Delta_i} \hat{W}_{\gamma_i \sigma_i}^i$ – произведение W -функций дуг r_i -ой петли i -го порядка,

включающей в себя сток t , $1 \leq i \leq m$; $\prod_{\beta_j=1}^{B_j} \bar{W}_{\alpha_j \beta_j}^j$ – произведение

W -функций дуг α_j -ой петли j -го порядка, не включающей в себя сток t , $1 \leq j \leq \ell$.

Далее на девятом этапе при переходе от эквивалентной W -функции $W_E(s)$ GERT-сети к ее характеристической функции $X_E(\zeta)$ используется формула Меллина:

$$f(x) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} X_E(\zeta) e^{\zeta x} d\zeta. \quad (4)$$

Характеристическая функция $X_E(\zeta)$ находится на основе топологического уравнения Мейсона путем замены в эквивалентной

производящей функции моментов $M_E(s)$ переменной s на $i\zeta$, где ζ – действительная переменная.

В [6] отмечено, что для обеспечения условий интегрирования в подынтегральное выражение уравнения (4) необходимо добавить множитель $e^{(-0,5\zeta^2)}$. С целью адекватного описания данной операции в структуре многослойной GERT-сети добавляется последовательная ветвь, описываемая нормально распределенной случайной величиной ζ^2 с нулевым математическим ожиданием и дисперсией, равной единице. Вновь образованную ("фиктивную") ветвь можно включить сразу после источника S сети. Тогда вновь определенная характеристическая функция $\tilde{X}_E(\zeta)$ определяется как: $\tilde{X}_E(\zeta) = e^{(-0,5\zeta^2)} X_E(\zeta)$.

Переходя от эквивалентных $W_E(s)$ функций к характеристическим $X_E(\zeta)$, на основании выражения (3) можно получить следующее аналитическое выражение:

$$X_E(\zeta) = \frac{\frac{1}{P_E} \sum_{\gamma_1=1}^{\Delta_1} \prod_{\sigma_1=1}^{\Delta_1} \hat{p}_{\gamma_1\sigma_1} \hat{X}_{\gamma_1\sigma_1}^1 + \dots - (-1)^m \sum_{\gamma_m=1}^{\Gamma_m} \prod_{\sigma_m=1}^{\Delta_m} \hat{p}_{\gamma_m\sigma_m} \hat{X}_{\gamma_m\sigma_m}^m}{1 - \sum_{\alpha_1=1}^{\Delta_1} \prod_{\beta_1=1}^{B_1} \bar{p}_{\gamma_1\sigma_1} \bar{X}_{\alpha_1\beta_1}^1 + \dots + (-1)^\ell \sum_{\alpha_\ell=1}^{A_\ell} \prod_{\beta_m=1}^{B_\ell} \bar{p}_{\gamma_m\sigma_m} \bar{X}_{\alpha_\ell\beta_\ell}^\ell}, \quad (5)$$

где $\prod_{\sigma_1=1}^{\Delta_1} \hat{p}_{\gamma_1\sigma_1}$ и $\prod_{\beta_m=1}^{B_\ell} \bar{p}_{\gamma_m\sigma_m}$ находятся из отношений

$$\prod_{\sigma_1=1}^{\Delta_1} \hat{p}_{\gamma_1\sigma_1} = \frac{\prod_{\sigma_1=1}^{\Delta_1} \hat{W}(s)_{\gamma_1\sigma_1}^1}{\prod_{\sigma_1=1}^{\Delta_1} \hat{M}(s)_{\gamma_1\sigma_1}^1} \quad \text{и} \quad \prod_{\beta_m=1}^{B_\ell} \bar{p}_{\gamma_m\sigma_m} = \frac{\prod_{\beta_m=1}^{B_\ell} \bar{W}(s)_{\sigma_\ell\beta_\ell}^\ell}{\prod_{\beta_m=1}^{B_\ell} \bar{M}(s)_{\sigma_\ell\beta_\ell}^\ell} \quad \text{заменой } s \rightarrow i\zeta \text{ [6].}$$

Следует отметить, что все математические операции, выполняемые на этапах 9 – 11, проанализированы, описаны в работах [4 – 8], прогнозируемы и, несмотря на сложность выполнения, не требуют дополнительного исследования.

Методика эквивалентных, упрощающих преобразований GERT-сети. Одним из основных этапов математического моделирования многослойных GERT-структур является этап эквивалентного

преобразования. При этом перед разработчиками встает сложная задача: при максимальной простоте разрабатываемой математической модели добиться минимизации погрешностей получаемых результатов.

Процедура преобразования многослойной GERT-сети к эквивалентной дуге представляется набором элементарных операций преобразования, в результате которых можно получить эквивалентные характеристические функции. Представим основные упрощающие преобразования.

1. Последовательные дуги. Если последовательно соединенные дуги многослойной GERT-сети имеют W -функции W_1 и W_2 то их эквивалентная W -функция $W_{E_{1,2}}$ вычисляется с помощью выражения: $W_{E_{1,2}} = W_1 W_2$. Эквивалентная дуга $X_{E_{1,2}}$ математически может описываться характеристической функцией [6]:

$$X_{E_{1,2}} = \operatorname{Re} \chi_1 \operatorname{Re} \chi_2 - \operatorname{Im} \chi_1 \operatorname{Im} \chi_2 + i(\operatorname{Re} \chi_1 \operatorname{Im} \chi_2 + \operatorname{Im} \chi_1 \operatorname{Re} \chi_2). \quad (6)$$

2. Параллельные дуги. Для дуг многослойной GERT-сети с вероятностями выбора соответственно p_1 и p_2 эквивалентная W -функция $W_{E_{1,2}}$ вычисляется с помощью выражения: $W_{E_{1,2}} = p_1 W_1 + p_2 W_2$, а характеристическая функция $X_{E_{1,2}}$ эквивалентной дуги описывается выражением [6]:

$$X_{E_{1,2}} = p_1 \operatorname{Re} \chi_1 + p_2 \operatorname{Re} \chi_2 + i(p_1 \operatorname{Im} \chi_1 + p_2 \operatorname{Im} \chi_2). \quad (7)$$

3. Дуга и петля первого порядка, соединяющая выход и вход узла. Если $W_1 = p_1 M_1$ есть W -функция петли первого порядка, соединяющей выход и вход узла, и имеющей вероятность выбора p_1 , а $W_2 = p_2 M_2$ является W -функцией дуги, выходящей из узла, и имеющей вероятность выбора p_2 , то эквивалентная W -функция этого фрагмента $W_{E_{1,2}}$

вычисляется с помощью выражения: $W_{E_{1,2}} = \frac{W_2}{1 - W_1}$, а вероятность $p_{E_{1,2}}$

перехода (дуги) $W_{E_{1,2}}$ равна: $p_{E_{1,2}} = \frac{p_2}{1 - p_1}$, при условии что $p_1 + p_2 \neq 1$.

Эквивалентная дуга $X_{E_{1,2}}$ описывается характеристической функцией [6]:

$$X_{E_{1,2}} = \frac{p_2(\operatorname{Re}\chi_2 - p_1 \operatorname{Re}\chi_1 \operatorname{Re}\chi_2 - p_1 \operatorname{Im}\chi_1 \operatorname{Im}\chi_2)}{(1 - p_1 \operatorname{Re}\chi_1)^2 + p_1^2(\operatorname{Re}\chi_1)^2} + \quad (8)$$

$$+ \frac{ip_2(\operatorname{Im}\chi_2(1 - p_1 \operatorname{Re}\chi_1) + p_1 \operatorname{Im}\chi_1 \operatorname{Im}\chi_2)}{(1 - p_1 \operatorname{Re}\chi_1)^2 + p_1^2(\operatorname{Im}\chi_1)^2}.$$

Для эквивалентных преобразований многослойной GERT-сети и приведения ее к единственной эквивалентной дуге воспользуемся следующим алгоритмом.

Входными данными приведенного алгоритма является структура сформированной многослойной GERT-сети в составе: множества узлов сети – $V = \{v_1, v_2, \dots, v_{k-1}, v_k, v_{k+1}, \dots, v_h\}$, множества дуг одного уровня сети – $D = \{d_{1,1}, d_{1,2}, \dots, d_{k-1,k}, d_{k,k}, d_{k,k+1}, \dots, d_{h-1,h}, d_{h,h}\}$, множества межуровневых дуг – $Dm = \{dm_{i,j}\}$.

На первом шаге алгоритма необходимо провести выделение межуровневых дуг $dm_{i,j}$ в качестве границ внутренних подсетей, требующих первоначального эквивалентного преобразования.

В случае успешного прохождения первого шага, далее, на втором шаге алгоритма, производится исключение петель первого рода путем пересчета характеристических функций дуг $d_{k,k+1}, \dots, d_{k,h}$, выходящих из некоторого узла v_k , по формуле (8).

Следует заметить, что введение в начальные входные данные и условия многоуровневости моделируемой структуры заставляют в цикле осуществлять проверку факта формирования упрощенной многослойной GERT-сети. В случае положительного ответа на этот вопрос в соответствии с алгоритмом выполняется шестой шаг – замена сформированных межуровневых дуг на эквивалентные, с пересчетом характеристических функций. На третьем шаге алгоритма производится дублирование узлов, имеющих две или более выходных дуги, с копированием существующих в GERT-сети или определенных после первого шага входных дуг. На четвертом шаге производится замена последовательных дуг на эквивалентные с исключением определенного ранее, внутреннего (v_k) узла эквивалентной дуги.

Выполнение первых четырех шагов алгоритма эквивалентного преобразования GERT-сети может привести к упорядочению и образованию совокупности последовательных и параллельных дуг, которые на пятом шаге алгоритма могут быть заменены на эквивалентные с пересчетом характеристических функций с помощью выражений (6) (7). В результате пошагового выполнения алгоритма должна сформироваться упрощенная

GERT-сеть, состоящая из двух узлов и одной эквивалентной дуги. Сложность предложенного алгоритма приблизительно составляет $O(n)^4$.

Выводы. Таким образом, разработана методика математического моделирования защищенной ИТС на основе многослойной GERT-сети, которая отличается от известных учетом многоуровневости существующих информационно-телекоммуникационных сетей.

Список литературы: 1. Вишневецкий В.М. Теоретические основы проектирования компьютерных сетей / В.М. Вишневецкий. – М.: Техносфера, 2003. – 512 с. 2. Кузнецов О.О. Протоколы защиты информации у компьютерных системах та мережах: Навч. посібник / О.О. Кузнецов, С.Г. Семенов. – Харків: ХНУРЕ, 2009. – 186 с. 3. Майника Э. Алгоритмы оптимизации на сетях и графах / Э. Майника. – 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, Я.В. Илюшко // "Системы озброєння і військова техніка. – Х.: ХУ ПС. – 2011. – Вип. 3 (27). – С. 64-67. 5. Семенов С.Г. Моделирование защищенного канала связи с использованием экспоненциальной GERT-сети / С.Г. Семенов, А.А. Можжаев // Информатика, математическое моделирование, экономика: Сб. научных статей. – Смоленск: Смоленский филиал АНО ВПО ЦС РФ "Российский университет кооперации". – 2012. – Том. 1. – С. 152-160. 6. Шибанов А.П. Обобщенные GERT-сети для моделирования протоколов, алгоритмов и программ телекоммуникационных систем: дис. ... доктора техн. наук: 05.13.13 / Шибанов Александр Петрович. – Рязань, 2003. – 307 с. 7. Pritsker A. A. B. Modeling and analysis using Q-GERT networks New York: Wiley: Distributed by Halsted Press, 1979. – 435 p. 8. Pritsker A.A.B., Happ W.W. GERT: Graphical Evaluation and Review Technique. Part I. Fundamentals // The Journal of Industrial Engineering (May 1966). – P. 67-101.

Статью представил д.т.н., профессор НТУ "ХПИ" Обод И.И.

УДК 651.326

Методика математичного моделювання захищеною ІТС на основі багатопарової GERT-мережі / Семенов С.Г. // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2012. – № 62 (968). – С. 185 – 193.

На основі теоретико-графового підходу моделювання розроблена методика математичного моделювання захищеної інформаційно-телекомунікаційної системи у вигляді багатопарової GERT-мережі. Визначені найбільш складні з обчислювальної точки зору етапи моделювання. Розроблений алгоритм еквівалентних, спрощуючих перетворень GERT-мережі. Бібліогр.: 8 назв.

Ключові слова: математична модель, GERT-мережа, захищена ІТС.

UDC 651.326

Methodology of mathematical design protected ITS, but to basis of multi-layered GERT-network / Semenov S.G. // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2012. – №. 62 (968). – P. 185 – 193.

On the basis of count approach design methodology of mathematical design the protected informatively-telecommunication system is worked out, as the multi-layered GERT-network. The most difficult from the calculable point of view stages of design are certain. The algorithm of equivalent, simplifying transformations of GERT-network is worked out. Refs.: 8 titles.

Keywords: mathematical model, GERT- network, protected ITS.

Поступила в редакцію 09.09.2012

ISSN 2079-0031 Вестник НТУ "ХПИ", 2012, № 62 (968)