IV международная научная школа
«Управление инцидентами и противодействие целевым киберфизическим атакам в распределенных крупномасштабных критически важных системах»
(IM&CTCPA-2018)

Применение метода топологического преобразования стохастических сетей для решения задач информационной безопасности

Лектор: профессор кафедры «Электрическая связь»
Петербургского государственного университета
путей сообщения
доктор военных наук, профессор
Привалов Андрей Андреевич

Санкт-Петербург
2018

Рассматриваемые вопросы:

1.Краткая историческая справка.

2. Сущность и содержание метода ТПСС:

- стохастические сети и их элементы;
- виды стохастических сетей;
- методы определения функции распределения времени реализации процесса, представленного в виде стохастической сети;
- определение параметров случайного процесса, представленного в виде стохастической сети;
- анализ результатов моделирования.

3. Примеры решения задач в области информационной безопасности

Краткая историческая справка

- **1959-60 г.г.** – Samuel J.Mason, Henry J. Zimmerman: - исследование топологии электрических схем, топологическое уравнение передачи тока и напряжения электрических цепей;
- **1965-66 г.г.** – Pritsker A.A.B., Harp W.W., Whitehouse G.E.: - приложения теории потоковых графов к исследованию временных процессов в системах с обратной связью, разработка метода GERT;
- **1966 г.** – меморандум RM-4973 NASA под общей редакцией Pritsker A.A.B.,содержащий полное системное описание GERT и имеющий целью разработки механизма согласования работ, выполняемых по программе “Appolo space system”;
- **1972-1982 г.г.** – Г.П. Захаров: - приложения метода GERT (ТПСС) для исследования систем связи;
- **1982 г.** - н./в. – дальнейшее развитие метода и его использование для исследования сложных организационно-технических и конфликтующих систем

Стохастические сети и их элементы

Стохастическая сеть - совокупность взаимоувязанных узлов (вершин) и ветвей, соединение которых соответствует алгоритму функционирования исследуемой системы. При этом сеть реализуется, если будет выполнено некоторое подмножество ветвей, время реализации которых выбирается в соответствии с вероятностным распределением.

***Логические Узлы*:**

$p_{РУi}$ - вероятность реализации узла;

Ветви: $t_{рвij}$; $p_{ввij}$; $f_{ij}(t)$; $f_{ij}(s)$

$p_{ввij}$ - вероятностью того, что данная ветвь будет выбрана при условии реализации вершины из которой она исходит;

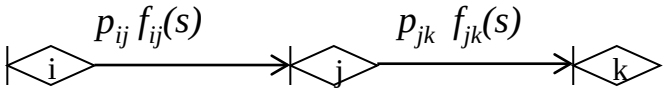
$$f_{ij}(s) = \int_0^{\infty} e^{-st} f_{ij}(t) dt$$

Виды стохастических сетей.

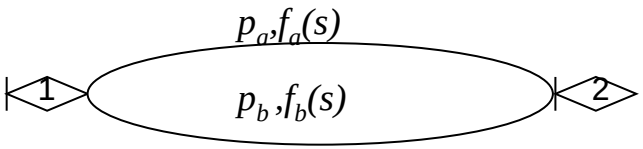
Эквивалентной называется функция, ставящая в соответствие случайному времени реализации сети его условную производящую функцию моментов, определяемую с использованием уравнения Мейсона для замкнутых графов.

Простые стохастические сети:

Стохастическая сеть, состоящая из ветвей описывающих элементарные физические процессы и логических узлов одного типа называется ***простой стохастической сетью****.*

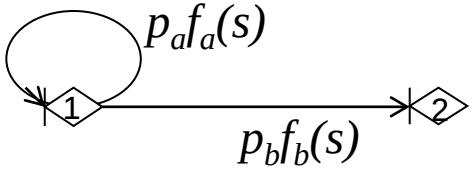


$$Q_{ik}(s) = p_{ij}\, f_{ij}(s)\, p_{jk} f_{jk}(s); \qquad (1)$$



$$Q_{12}(s) = p_a\, f_a(s) + p_b\, f_b(s); \quad p_a + p_b = 1; \qquad (2)$$

Связная замкнутая последовательность ориентированных ветвей стохастической сети, каждая вершина которых является общей ровно для двух ветвей (или ветви), соединяющих вершину саму с собой, называется ***петлей.***



$$Q_{12}(s) = \frac{p_b\, f_b(s)}{1 - p_a\, f_a(s)};$$

Петлей k-го порядка *называется множество* ***k*** *не связанных между собой петель первого порядка.*

$$Q_k(s) = \prod_{i=1}^{k} Q_i(s); \qquad (4) \qquad \mathrm{H} = 1 + \sum_{\mathrm{k}=1}^{\mathrm{K}} (-1)^{\mathrm{k}} Q_k(s) = 0; \qquad (5)$$

Виды стохастических сетей.

Порядок определения эквивалентной функции простой стохастической сети:

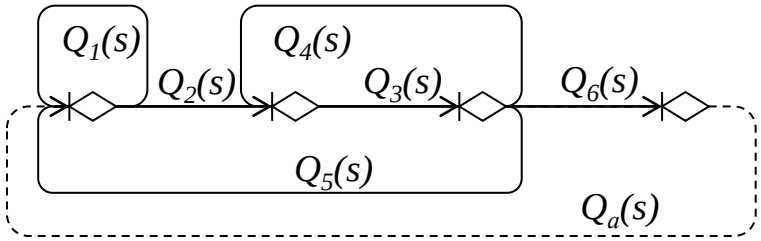


Рис. 1

1. Замкнуть стохастическую сеть фиктивной ветвью, исходящей из последнего (выходного) узла и входящей в первый (входящий) узел. На рис.1 эта ветвь показана пунктиром и характеризуется функцией $Q_a(s)$.

2. Определить все петли ***k***-го порядка:

- петли первого порядка: $Q_1(s);\ Q_3(s)Q_4(s);\ Q_2(s)Q_3(s)Q_5(s);$ и $Q_2(s)Q_3(s)Q_6(s)Q_a(s);$
- петля второго порядка: $Q_1(s)Q_3(s)Q_4(s).$

3. С использованием топологического уравнения определить эквивалентную функцию сети. Помня, что $Q(s) = [Q_a(s)]^{-1}$ из топологического уравнения получаем

$$H=1-Q_1(s)-Q_3(s)Q_4(s)-Q_2(s)Q_3(s)Q_5(s)-Q_2(s)Q_3(s)Q_6(s)Q^{-1}(s)+\ Q_1(s)Q_3(s)Q_4(s)=0.$$

Отсюда:

$$Q(s)=\frac{Q_2(s)Q_3(s)Q_6(s)}{1-Q_1(s)-Q_3(s)Q_4(s)-Q_2(s)Q_3(s)Q_5(s)+Q_1(s)Q_3(s)Q_4(s)}.$$

Виды стохастических сетей

Сложные стохастические сети.

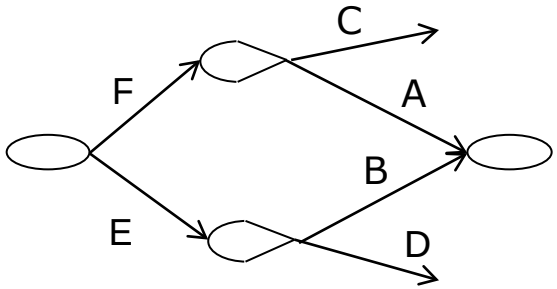
Стохастическая сеть, состоящая из ветвей, представляющих в данной сети сложные (композиционные) процессы и/или содержащая различные типы логических узлов называется сложной.

Виды сложных стохастических сетей:

- *Укрупненные стохастические сети;*
- *Смешанные стохастические сети;*
- *укрупненные смешанные стохастические сети;*

Логический узел «И»:

$p_A;\ p_B;\ p_D = 1 - p_A,\ p_C = 1 - p_B;\ p_E = p_F = 1.\ t_A;\ t_B;\ t_C;\ t_D;\ t_E = t_F = 0.$

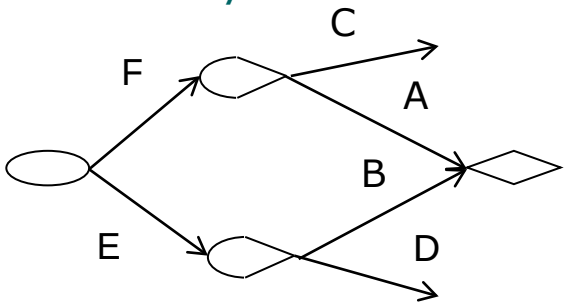


$$Q_{Ие}(s) = \frac{a}{a+s} + \frac{b}{b+s} - \frac{a+b}{a+b+s};\ a = \frac{1}{t_A};\ b = \frac{1}{t_B}; \qquad (1)$$

$$Q_{И\gamma}(s) = \left(\frac{\lambda}{\lambda+s}\right)^{\kappa};\quad \lambda = \frac{T_\gamma}{D\gamma};\quad \kappa = \frac{T_\gamma^2}{D\gamma}; \qquad (2)$$

$$T_\gamma = \int_0^\infty td\left[\Upsilon_A(\mu t,\alpha)\Upsilon_B(\nu t,\beta)\right]; D_\gamma = \int_0^\infty (t-T_\gamma)^2 d\left[\Upsilon_A(\mu t,\alpha)\Upsilon_B(\nu t,\beta)\right];$$

Логический узел «ИЛИ»:



$$Q_{ИЛИе}(s) = \frac{a+b}{a+b+s};\ a = \frac{1}{t_A};\ b = \frac{1}{t_B}; \qquad (3)$$

$$Q_{ИЛИ\gamma}(s) = \left(\frac{\mu}{\mu+s}\right)^{\alpha} + \left(\frac{\nu}{\nu+s}\right)^{\beta} - \left(\frac{\lambda}{\lambda+s}\right)^{\kappa}; \qquad (4)$$

Методы определения функции распределения времени реализации процесса, представленного в виде стохастической сети

Теорема. *Стохастическая сеть, соответствующая стационарному случайному процессу имеет эквивалентную функцию, голоморфную при Re s ‹ 0.*

1. Метод двух-моментной аппроксимации

$$M_k = (-1)^k \frac{d^k}{ds^k}\left[\frac{Q(s)}{Q(0)}\right]_{s=0}; \quad \bar{t}_П = -\frac{d}{ds}\left[\frac{Q(s)}{Q(0)}\right]_{s=0}; \quad D[t_П] = \frac{d^2}{ds^2}\left[\frac{Q(s)}{Q(0)}\right]_{s=0} - \left\{-\frac{d}{ds}\left[\frac{Q(s)}{Q(0)}\right]_{s=0}\right\}^2;$$

$$F(t) = \begin{cases} 0, t < 0; \\ \int_0^t \frac{\mu^\alpha}{\Gamma(\alpha)} x^{\alpha-1} \exp[-\mu x] dx, t \geq 0, \end{cases} \qquad \alpha = \frac{\overline{t_П}^2}{D[t_П]}; \quad \mu = \frac{\overline{t_П}}{D[t_П]};$$

2. Метод четырех-моментной аппроксимации

Сущность метода заключается в определении первых четырех центральных моментов случайного времени реализации сети с последующим расчетом значений параметров семейства распределений Пирсона и выбором типа распределения из одиннадцати возможных.

Методы определения функции распределения времени реализации процесса, представленного в виде стохастической сети

3. Метод обращения

1) Эквивалентная функция Q(s) является рациональной алгебраической функцией.

Разложение Хевисайда

$$Q(s)=\frac{f(s)}{\varphi(s)};\ \deg[f(s)]=m;\ \deg[\varphi(s)]=n;\ n>m;$$

а) $$\varphi(s)=a_0(s-s_1)(s-s_2)\ldots(s-s_i)\ldots(s-s_n),\ s_i\neq s_{i+1},\ i=\overline{1,n};$$

$$Q(s)=\sum_{i=1}^{n}\frac{f(s_i)}{\varphi'(s_i)}\cdot\frac{1}{s-s_i};\qquad L^{-1}[Q(s)]=f(t)=\sum_{i=1}^{n}\frac{f(s_i)}{\varphi'(s_i)}\cdot\exp[s_i t];$$

б) $$\varphi(s)=a_0(s-s_1)^{a_1}(s-s_2)^{a_2}\ldots(s-s_i)^{a_i}\ldots(s-s_n)^{a_n},\ s_i\neq s_{i+1},\ i=\overline{1,n};$$

$$L^{-1}[Q(s)]=f(t)=\sum_{i=1}^{n}\sum_{j=1}^{a_i}\frac{t^{a_i-j}\exp(s_i t)}{(j-1)!(a_i-j)!}\cdot\frac{d^{j-1}}{ds^{j-1}}\left[\frac{f(s)(s-s_i)^{a_i}}{\phi(s)}\right]_{s=s_i}.$$

Разложение на простые дроби

$$\frac{f(s)}{\varphi(s)}=\sum_{i=1}^{n}\sum_{j=1}^{a_i}\frac{b_{kj}}{(s-s_k)^j};$$

Кратность корней s_i равна a_i.

Методы определения функции распределения времени реализации процесса, представленного в виде стохастической сети

2. Эквивалентная функция представляет собой сложную или неявнозначную функцию

а) разложение эквивалентной функции ***Q(s)*** в ряд по отрицательным степеням ***s***

$$Q(s)=\frac{b_1}{s}+\frac{b_2}{s}+\dots.;\quad \text{при } |s|>0:\quad f(t)=L^{-1}[Q(s)]=b_1+b_2t+\frac{b_3}{2!}t^2+\dots+\frac{b_k}{(k-1)!}t^{k-1}+\dots$$

б) асимптотическое разложение изображения

при $s\to\infty$ $$Q(s)\sim\sum_{j=0}^{\infty}c_j\frac{\Gamma(\lambda_{j+1})}{s^{\lambda_j}};\quad f(t)=\sum_{j=0}^{\infty}c_jt^{\lambda_j},\quad -1<\lambda_0<\lambda_1<\lambda_2<\dots<\lambda_j<\dots.$$

б) асимптотическое разложение оригинала

Если: Q(s) имеет лишь изолированные особые точки – полюсы и алгебраические точки разветвления;
Q(s) в полуплоскости *Re(s) < 0* стремится к нулю при $|s|\to\infty$;
число особых точек $s=s_k$ с наибольшей действительной частью конечно ($k = 1,l$)
и разложение *Q(s)* в окрестности каждой такой точки задается рядом

$$\sum_{j=0}^{\infty}c_j^{(k)}(s-s_k)^{\lambda_j^{(k)}};\quad -N_k<\lambda^{(k)}{}_0<\lambda^{(k)}{}_1<\dots<\lambda^{(k)}{}_j<\dots,$$

то, при $t\to\infty$ $$f(t)\sim\sum_{k=1}^{l}\exp(s_kt)\sum_{j}^{\infty}\frac{c_j^{(k)}}{\Gamma(-\lambda_j^{(k)})t^{\lambda_j^{(k)}+1}}.$$

$$F(t)=\int_0^t f(x)dx;\qquad \bar{t}_{\Pi}=\int_0^{\infty}tf(t)dt;\qquad D[t_{\Pi}]=\int_0^{\infty}t^2f(t)dt-\overline{t}_n^{\,2}.$$

Определение параметров случайного процесса, представленного в виде стохастической сети

Теорема: *Если стохастическая сеть имеет голоморфную дробно-рациональную эквивалентную функцию $Q_э(s) = f(s)/\varphi(s)$, то анализируемый случайный процесс является стационарным со спектральной плотностью, определяемой по формуле*

$$Q(j\omega) = \sum_{i=1}^{n} \frac{f(s_i)}{\phi'(s_i)} \cdot \frac{1}{|s_i| + j\omega}, \qquad (1)$$

где s_i – простые полюса эквивалентной функции.

Теорема: *Закон распределения времени свершения процесса, моделирование которого приводит к неограниченному укрупнению стохастической сети сходится к нормальному, а сам моделируемый процесс является гауссовым.*

$$Q(j\omega) = \sum_{i=1}^{n} \frac{f(s_i)}{\phi'(s_i)} \cdot \frac{1}{|s_i| + j\omega} = \sum_{i=1}^{n} \frac{f(s_i)\exp\{-j \cdot arctg[\frac{\omega}{s_i}]\}}{\phi'(s_i)\sqrt{|s_i|^2 + \omega^2}}; \qquad (2)$$

$$R(\tau) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} |Q(j\omega)|^2 \exp(i\omega\tau) d\omega = \frac{1}{2\pi} \int_{-\infty}^{\infty} \left| \sum_{i=1}^{n} \frac{f(s_i)}{\phi'(s_i)\sqrt{|s_i|^2 + \omega^2}} \right|^2 \exp(i\omega\tau) d\omega; \qquad (3)$$

$$\tau_0 = \frac{1}{2R(0)} \int_{0}^{\infty} |R(\tau)| d\tau; \qquad (4) \qquad D = R(0). \qquad (5) \qquad \Lambda_к = \frac{\sqrt{R''(0)}}{\pi} \qquad (6)$$

Определение параметров случайного процесса, представленного в виде стохастической сети

$$M[X(t)] = P(t \le T_з^*) \quad (1)$$

$$P[X(\tau)_з \ge P_з^*] = \Phi(-u); \quad (2)$$

$$M[\xi] = \xi\Phi(-u), \quad (3)$$

здесь $u = [P_з - X(\tau)] / \sigma_x$;

$$D[\xi] = \frac{\sigma_x^2}{\sin[arctg(\Delta P / M[\xi])]}; \quad (4)$$

$$\overline{T_u} = \frac{P[X(t) \ge P_з]}{\Lambda(P_з)}. \quad (5)$$

Анализ результатов моделирования

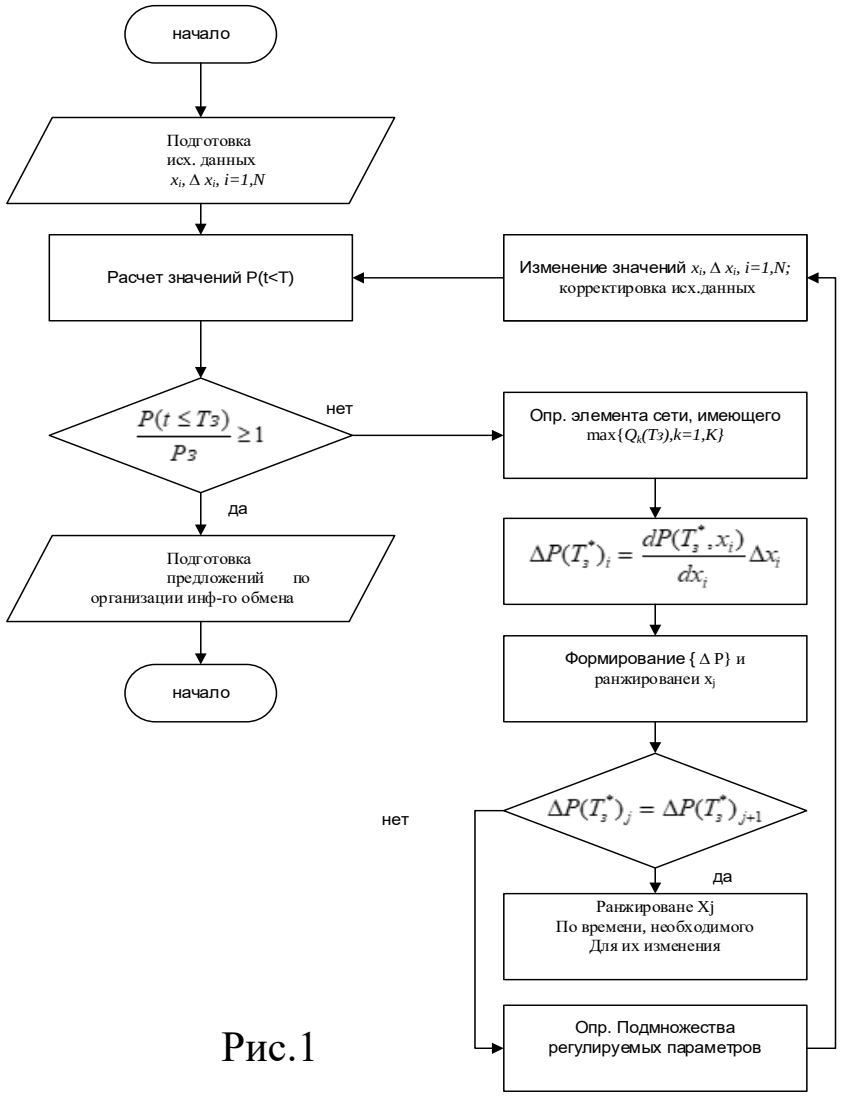


Рис.1

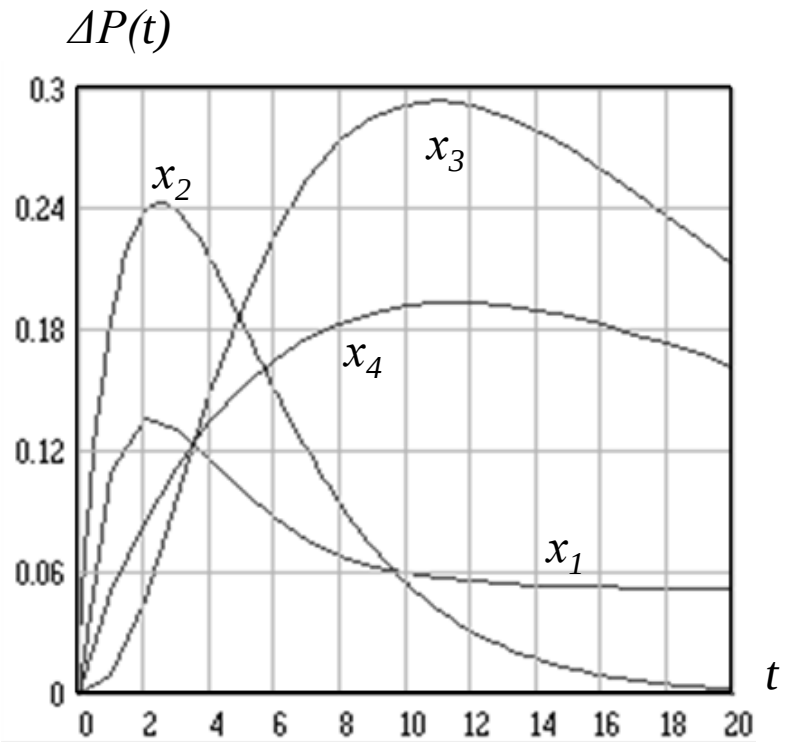
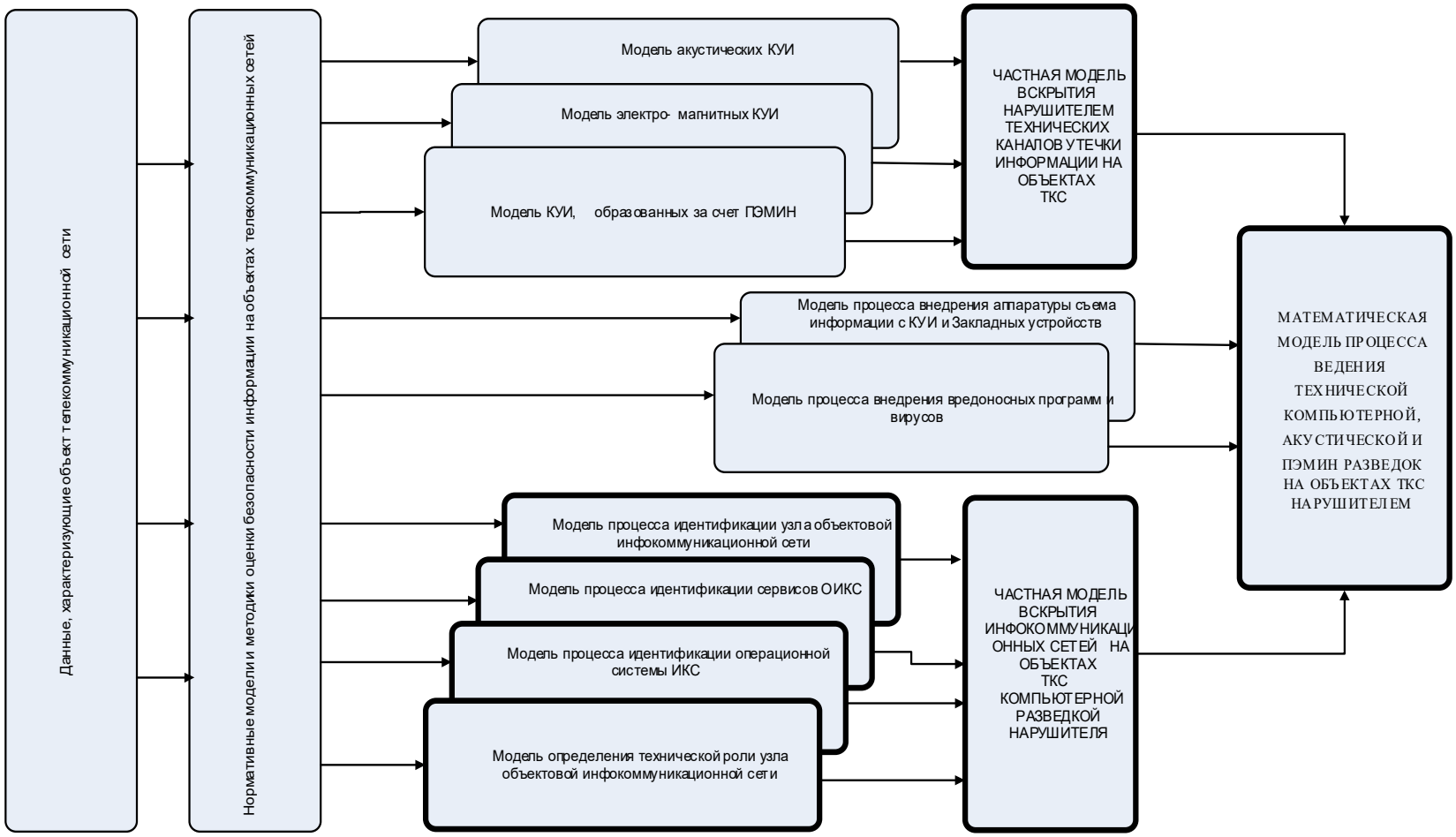


Рис.2

Примеры решения задач в области информационной безопасности

Обобщенная математическая модель процесса ведения технической компьютерной акустической и ПЭМИН разведок на объектах телекоммуникационных сетей нарушителем



Частная модель процесса вскрытия нарушителем технических каналов утечки информации на объектах телекоммуникационных сетей

(1)

где:

; ; ;

; ;

; (2)

где: ;

;

;

;

(3)

;

(4)

Рис. 1 Стохастическая сеть процесса вскрытия нарушителем технических каналов утечки информации

Исходные данные:

$t_b; t_r; t_k; t_c; t_c; P1, P2, P3$

Допущения:

- ф.р. Времени свершения процессов вскрытия и внедрения на ОТКС СН закладных устройств относятся к классу экспоненциальных;
- Вероятности доступности нарушителя к КУИ расчитываются по известным методикам в соответствии со структурой объекта ТКС СН;
- в качестве первоочередного нарушитель выбирает тот КУИ, к которому проще получить доступ для проведения измерений и установки закладного устройства;
- нарушитель явдяется хорошо подготовленным специалистом и располагает необходимой для производства измерений аппаратурой.

Частная математическая модель вскрытия инфокоммуникационной сети на объекте телекоммуникационной сети системой компьютерной разведки

Рис. 1 Укрупненная стохастическая сеть вскрытия ИКС на ОТКС системой КР

Рис 2. Стохастическая сеть процесса идентификации узла ОИКС

Рис.3 Стохастическая сеть процесса идентификации сервисов

Рис 4. Стохастическая сеть процесса идентификации операционной системы

Рис 5. Стохастическая сеть процесса определения технической роли узла в ОИКС

Исходные данные:

$P_{дост}$; $P_{обСЗ}$; $P_{порт}$; $P_{скр\,серв}$; $P_{пз}$; $P_{скр\,ОС}$; $P_{РУ}$; $a = 1/t_{скан}$, $b = 1/t_{п}$; $a_2 = 1/t_{ск\,пр}$, $b_2 = 1/t_{п2}$, $f_1 = 1/t_{ан1}$; $a_3 = 1 / t_{пз}$, $f_2 = 1 / t_{ан2}$; $d = 1 / t_{ппи}$; $f_3 = 1 / t_{ан3}$; $t_{ппр}$; $t_{прс}$; $t_{нпр}$; $t_{прс}$; $t_{обз}$; $t_{ппи}$; $t_{ан2}$ N; M; $N_{порт}$; $M_{порт}$; $N_{ТЗ}$;

$$t_{скан} = Nt_{прс} / 2 + M(t_{ппр} + t_{прс} / 2) ; \quad (1)$$

$$t_{ск\,пр} = N_{порт}t_{прс} / 2 + M_{порт}(t_{ппр} + t_{прс} / 2); \quad (2)$$

$$t_{пз} = N_{ТЗ}(t_{обз} + t_{прс}); \quad (3)$$

$$(4)$$

Обобщенная математическая модель процесса ведения технической компьютерной, акустической и ПЭМИН разведок на объектах телекоммуникационных сетей нарушителем

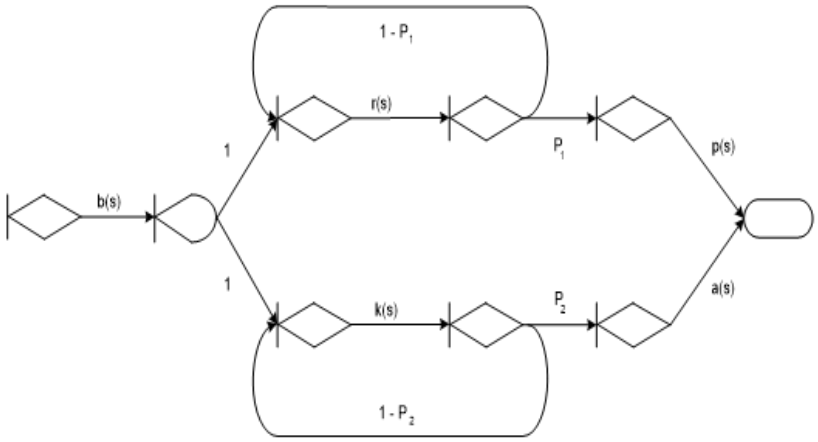


Рис.1 Стохастическая сеть процесса ведения нарушителем ТКАПР и внедрения вредоносных программ и установки закладных устройств на объекте ТКС

$$Q(s) = b(s)\left[\frac{p(s)r(s)P_1}{1-(1-P_1)r(s)} + \frac{k(s)a(s)P_2}{1-(1-P_2)k(s)} - \frac{p(s+y)r(s+y)P_1}{1-(1-P_1)r(s+y)} - \frac{k(s+x)a(s+x)P_1}{1-(1-P_1)k(s+x)}\right]/Q(0), \quad (1)$$

где:

$$\chi = -\frac{d}{ds}\left[\frac{p(s)r(s)P_1}{1-(1-P_1)r(s)}\right]_{s=0}^{-1}; \qquad y = -\frac{d}{ds}\left[\frac{k(s)a(s)P_2}{1-(1-P_2)k(s)}\right]_{s=0}^{-1};$$

$$f(t) = [\varphi_1(t) - \varphi_3(t) + \varphi_2(t) - \varphi_4(t)]/Q(0); \quad (2)$$

где:

$$\varphi_1(t) = \sum_{i=1}^{3} \frac{p\cdot P_1\cdot b\cdot r\cdot exp(s_{\varphi 1i}\cdot t)}{3\cdot s_{\varphi 1i}{}^2+2\cdot s_{\varphi 1i}\cdot B1+B2}; \quad \varphi_2(t) = \sum_{i=1}^{3} \frac{b\cdot P_2\cdot k\cdot a\cdot exp(s_{\varphi 2i}\cdot t)}{3\cdot s_{\varphi 2i}{}^2+2\cdot s_{\varphi 2i}\cdot A1+A2};$$

$$\varphi_3(t) = \sum_{i=1}^{3} \frac{p\cdot P_1\cdot b\cdot r\cdot exp(s_{\varphi 3i}\cdot t)}{3\cdot s_{\varphi 3i}{}^2+2\cdot s_{\varphi 3i}\cdot B3+B4}; \quad \varphi_4(t) = \sum_{i=1}^{3} \frac{k\cdot P_1\cdot b\cdot a\cdot exp(s_{\varphi 4i}\cdot t)}{3\cdot s_{\varphi 4i}{}^2+2\cdot s_{\varphi 4i}\cdot A3+A4};$$

$A1 = b + a + kP_2$; $A2 = ba + bkP_2 + akP_2$; $A3 = b + a + 3x + kP_2$;

$A4 = ab + 2bx + bkP_2 + 2xa + akP_2 + 3x^2 + 2xkP_2$; $B1 = b + p + rP_1$;

$B2 = bp + brP_1 + prP_1$; $B3 = b + p + 3y + rP_1$;

$B4 = pb + 2by + bpP_1 + 2yp + prP_1 + 3y^2 + 2yrP_1$;

$s_{\varphi 11} = -b$; $s_{\varphi 12} = -p$; $s_{\varphi 13} = -rP_1$; $s_{\varphi 21} = -b$; $s_{\varphi 22} = -a$; $s_{\varphi 23} = -kP_2$;

$s_{\varphi 31} = -(b+y)$; $s_{\varphi 32} = -(p+y)$; $s_{\varphi 33} = -(P_1 r + y)$; $s_{\varphi 41} = -(b+x)$;

$s_{\varphi 32} = -(a+x)$; $s_{\varphi 33} = -(P_2 k + x)$;

$$F(t) = \frac{1}{Q(0)}\left[\sum_{i=1}^{3}\frac{\Phi 1_i}{-s_{\varphi 1i}}(1-e^{s_{\varphi 1i}}) - \sum_{i=1}^{3}\frac{\Phi 3_i}{-s_{\varphi 3i}}(1-e^{s_{\varphi 3i}}) + \sum_{i=1}^{3}\frac{\Phi 2_i}{-s_{\varphi 2i}}(1-e^{s_{\varphi 2i}}) - \sum_{i=1}^{3}\frac{\Phi 4_i}{-s_{\varphi 4i}}(1-e^{s_{\varphi 4i}})\right]; \quad (3)$$

$$T = \frac{1}{Q(0)}\left[\sum_{i=1}^{3}\frac{\Phi 1_i}{s_{\varphi 1i}{}^2} - \sum_{i=1}^{3}\frac{\Phi 3_i}{s_{\varphi 3i}{}^2} + \sum_{i=1}^{3}\frac{\Phi 2_i}{s_{\varphi 2i}{}^2} - \sum_{i=1}^{3}\frac{\Phi 4_i}{s_{\varphi 4i}{}^2}\right] \quad (4)$$

Результаты моделирования процесса ведения технической компьютерной, акустической и ПЭМИН разведок на объектах телекоммуникационных сетей нарушителем

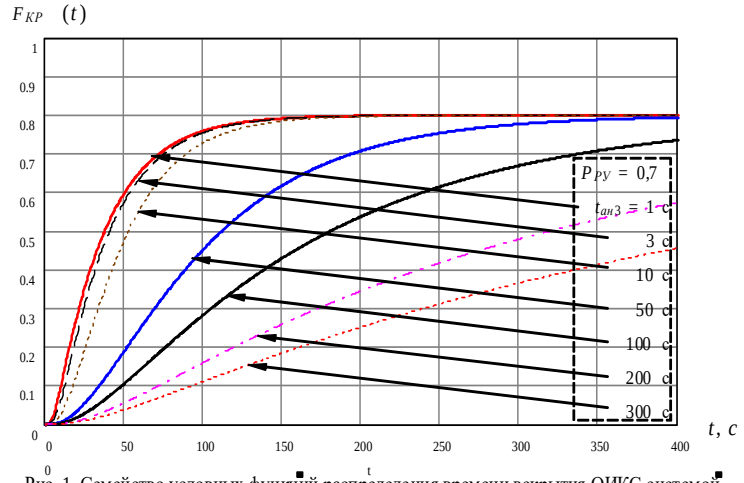


Рис. 1. Семейство условных функций распределения времени вскрытия ОИКС системой компьютерной разведки нарушителя при различном времени проведения анализа

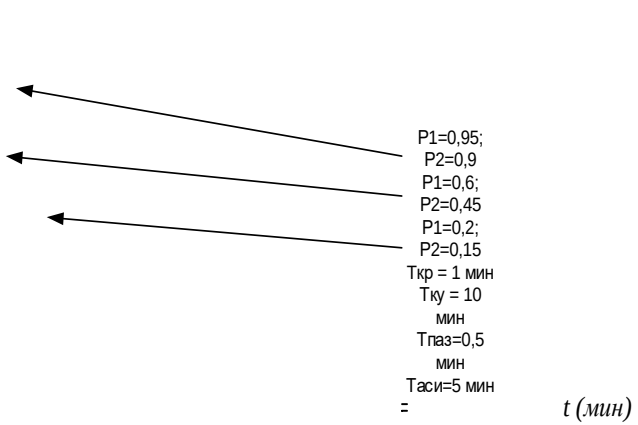


Рис.3 Семейство функций распределения времени вскрытия объекта ТКС Системой ТКАПР нарушителя при различных значениях вероятности доступности

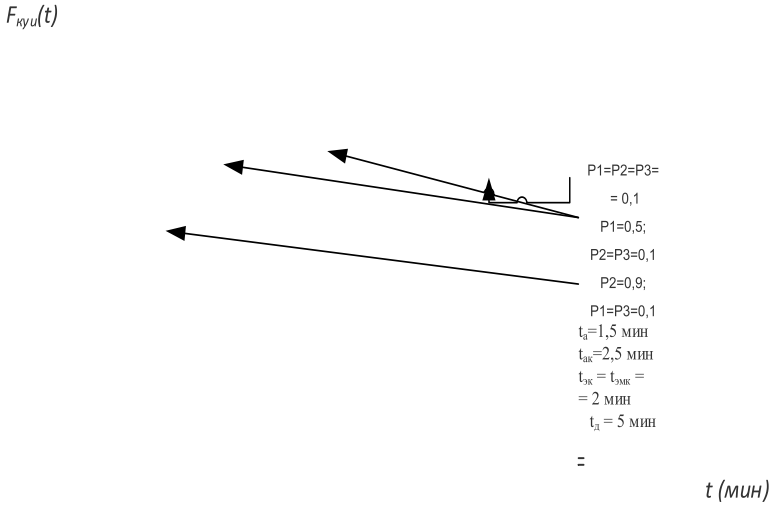


Рис.2 Семейство функций распределения времени вскрытия каналов утечки информации при различных значениях вероятности доступности нарушителя на объект ТКС для проведения измерений и установки закладных устройств

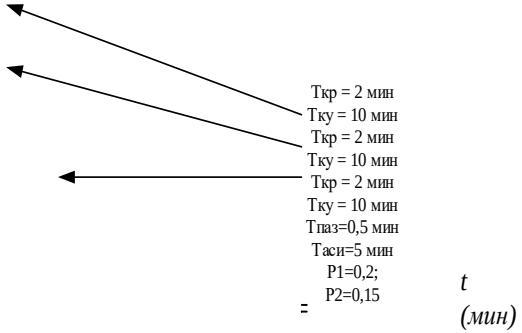


Рис.3 Семейство функций распределения времени вскрытия объекта ТКС системой ТКАПР нарушителя при различных значениях среднего времени реализации частных процессов ТКАПР

СПАСИБО ЗА ВНИМАНИЕ