ПРИМЕНЕНИЕ ТЕОРИИ МАРКОВСКИХ ЦЕПЕЙ ДЛЯ ПОСТРОЕНИЯ МОДЕЛИ ОПТИМИЗАЦИИ СОСТАВА КОМПЛЕКСОВ СРЕДСТВ ЗАЩИТЫ СОВРЕМЕННЫХ СИСТЕМ ПЕРЕДАЧИ И ОБРАБОТКИ ДАННЫХ

Есиков О.В., Кислицин А.С.

Тульский артиллерийский инженерный институт

300012, Тула, пр.Ленина 99, каф. “Математ. программного и информационного обеспечения АСУ”

Закрытое акционерное общество «ЛУКОЙЛ-ИНФОРМ»

101000, Москва, Сретенский бульвар 11

Предложен подход к построению математических моделей оптимизации состава комплексов средств защиты информации, основанный на применении теории марковских цепей. Получены зависимости для оценки эффективности функционирования систем защиты.

Пусть в системе передачи и обработки данных (СПОД), известного назначения и конфигурации, определены возможные цели злоумышленника и составлен полный перечень возможных угроз информации и средств их нейтрализации (средств защиты). Средства защиты нейтрализующие конкретную угрозу составляют рубеж защиты. Обозначим через M общее число угроз информации; A – множество номеров угроз информации; F – число возможных целей злоумышленников в СПОД; D – множество номеров средств защиты которые могут быть использованы в системе защиты; B_f – множество номеров угроз информации реализуемых злоумышленником при достижении f – й цели; N_j^f -множество номеров средств защиты, которые потенциально могут быть использованы для противодействия реализации злоумышленником f-й цели на j-м рубеже защиты (для нейтрализации j-й угрозы, входящей в f-ю цель) ($f = 1,2,\ldots,F$; $j = 1,2,\ldots,M$).

Причем, $B_f \subset A$, $\bigcup_{f=1}^{F} B_f = A$, $n_f = |B_f|$ и $\bigcup_{f=1}^{F} \bigcup_{j \in B_f,} N_j^f \subset D$.

Рассмотрим систему, в которой протекает марковский случайный процесс [1] с дискретными состояниями S_0, $S_1,\ldots, S_{n_f}, S_{n_f+1}$ ($f=1,2,3,\ldots,F$). Граф состояний системы представлен на рис.1. Каждое из состояний S_j ($j=1,2,\ldots,n_f$, $f=1,2,\ldots F$) соответствует реализации злоумышленником одной и только одной угрозы информации из множества B_f ($f=1,2,\ldots,F$). Реализация каждой из угроз информации заключается в преодолении злоумышленником соответствующего рубежа защиты и (или) совершении требуемых ему несанкционированных действий на этом рубеже.

Состояние S_0 соответствует началу работы злоумышленника по реализации своей цели (ни один рубеж защиты не преодолен); состояние S_j ($j=1,2,\ldots, n_f-1$) заключается в реализации злоумышленником j-й угрозы (преодолении j-го рубежа защиты); состояние S_{n_f} соответствует реализации злоумышленником f-й цели; состояние S_{n_f+1} – система защиты зафиксировала проникновение злоумышленника, и ею или службой безопасности предприняты соответствующие меры.

Для преодоления j-го рубежа при реализации f-й цели ($j = 1,2,\ldots,n_f$, $f=1,2,\ldots,F$) злоумышленник может использовать максимально до k_j^f попыток ($k_j^f = 1,2,3,\ldots$). При реализации каждой такой попытки система может перейти в следующее состояние (система защиты при этом деятельность злоумышленника не регистрирует), остаться в исходном состоянии, что соответствует неуспешной реализации данной попытки) или перейти в состояние n_f+1, соответствующее штатной реакции системы защиты на действия злоумышленника. Система переходит из i-го состояния в j-е в случае, если злоумышленник успешно преодолел (нейтрализовал) все средства защиты, составляющие j-й рубеж защиты. При этом система защиты действия злоумышленника не зарегистрировала.

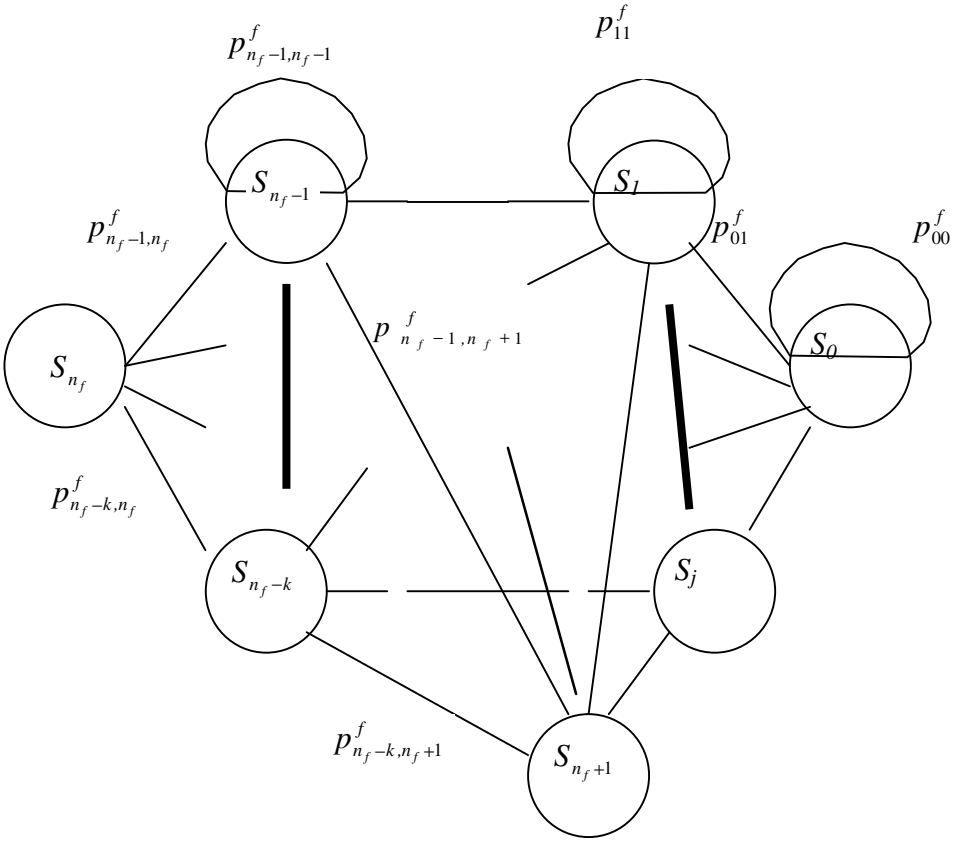

Рис. 1. Граф состояний системы

В начальный момент времени

$P_o^f(0)=1; P_j^f(0)=0 (j=1,2,...,n_f+1; f=1,2,...,F)$; $x_{jm}=0, \forall j,m; k_j^f=1, \forall j,f$,

где $x_{jm}=\{0,1\}$, $x_{jm}=1$, если m - е средство используется на j-м рубеже защиты, $x_{jm}=0$ – в противном случае, ($j \in B_f, j \neq 0, j \neq M+1$; $m \in N_j^f$); $P_j^f(l)$ - вероятность нахождения системы в состоянии S_j на l-м шаге.

В случае, когда переходные вероятности постоянны $p_{ij}^f(l)=const, (l=1,2,...,K_f)$, получим зависимости для определения вероятностей нахождения системы в каждом из состояний на l-м шаге ($l=1,2,...,K_f$).

$$P_o^f(l)=P_0^f(l-1)p_{00}^f;$$

$$P_j^f(l)=\sum_{\substack{i\in B_f,\\ i\neq M+1,\\ i\neq b_f^p}} P_i^f(l-1)p_{i,j}^f h_{ij}^f, \forall j \in B_f, j\neq 0,$$

где $h_{ij}^f=\begin{cases} g_j^f - \text{в случае } i\neq j \\ 1 - \text{в случае } i=j \end{cases}$,

K_f – общее число попыток преодоления злоумышленником системы защиты; g_j^f - вероятность преодоления j-го рубежа защиты при попытке достижения злоумышленником f-й цели

$$g_j^f=\left(1-e^{-q_j\omega_f}\right)\prod_{m\in N_j^f}\left(1-\rho_{jm}^f x_{jm}\right);$$

ρ_{jm}^f - вероятность успешного функционирования m-го средства защиты по противодействию деятельности злоумышленника на j-м рубеже при попытке реализации им f-й цели ($j \in B_f, j \neq 0, j \neq M+1$;$f=1,2,...,F$; $m \in N_j^f$); q_j-коэффициент согласования при переходе системы в j-е

состояние; ω_f -средний (максимальный/минимальный) уровень квалификации злоумышленника при реализации *f*-й цели, $\omega_f \in [0,1]$ при попытке реализации злоумышленником *f*-й цели (*f=1,2,…,F*); b_f^p -элемент множества B_f, соответствующий состоянию системы S_{n_f} .

Причем, $\sum_{j \in B_f} P_j^f(l) = 1, \forall l.$

При этом, эффективность функционирования системы защиты информации может оценена с помощью следующих параметров.

1. Средняя величина потерь СПОД от реализации злоумышленником всех целей.
2. Вероятность реализации злоумышленником всех целей.
3. Вероятность успешного противодействия системы защиты действиям злоумышленника по реализации всех своих целей.
4. Общая стоимость системы защиты.

Значения данных величин могут быть определены по следующим зависимостям.

1. Средний объем потерь от деятельности злоумышленника при достижении им всех целей

$$C^p = \sum_{f=1}^{F} \sum_{l=1}^{K_f} \sum_{\substack{j \in B_f, \\ j \neq 0, \\ j \neq M+1}} P_j^f(l) c_{jf} ,$$

где $c_{jf} = c^1_{jf} + c^2_{jf} + c^3_{jf}$;

c^1_{jf}, c^2_{jf}, c^3_{jf} – объем потерь системы от нарушения конфиденциальности информации, объем потерь от невыполнения ряда работ, стоимость восстановления системы защиты при реализации злоумышленником *j*-й угрозы при попытке достижения *f*-й цели соответственно.

2. Вероятность реализации всех целей злоумышленником

$$P^p = \prod_{f=1}^{F} \left(1 - \prod_{l=1}^{K_f} \left[1 - \sum_{\substack{j \in B_f, \\ j \neq b_f^p, \\ j \neq M+1}} P_j^f(l) p^f_{jb_f^p} h^f_{b_f^p} \right] \right)$$

3. Вероятность успешного противодействия системы достижению всех целей злоумышленником

$$P^з = \prod_{f=1}^{F} \left(1 - \prod_{l=1}^{K_f} \sum_{\substack{j \in B_f, \\ j \neq M+1}} P_j^f(l) \right) \cdot$$

4. Общая стоимость системы защиты

$$C^з = \sum_{f=1}^{F} \sum_{\substack{j \in B_f, \\ j \neq 0, \\ j \neq M+1}} \sum_{m \in N_j^f} c^з_{jm} x_{jm} ,$$

где $c_{jm} = s^0_m + s^1_{jm}$ -стоимость использования *m*-го средства на *j*-м рубеже, s^0_m -стоимость *m*-го средства, s^1_{jm} -стоимость установки и обслуживания *m*-го средства на *j*-м рубеже защиты.

Литература

1. 1. Венцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. М.:Наука.-1991, 384 с.

APPLICATION OF THE MARKOV CHAINS THEORY TO CONSTRUCTION OF MODELS FOR CONTENT OPTIMIZATION OF PROTECTION MEANS COMPLEXES IN UP-TO-DATE DATA TRANSMISSION AND PROCESSING SYSTEMS

Esikov O.V., Kislitsin A.C.

The Tula Artillery Engineering Institute
300012, Tula, Prospekt Lenina 99, Chair: "Mathematical Code and Information Support for Computer-Aided Control Systems"
Closed Stock Company LUKOIL-INFORM, 101 000, Moscow, 11 Sretensky br.

Suppose in the data transmission and processing system (DTPS) of known designation and configuration there have been determined probable aims of an intruder and also produced a complete list of probable menaces to information and of means for their neutralization (protection means). The protection means neutralizing a concrete menace constitute a protection boundary. Let us denote with M the total number of menaces to the information; A is a set of numbers of menaces to the information; F is a number of probable intruder's aims in DRPS ; D is a set of numbers of protection means which can be used in the protection system; B_f is a set of numbers of menaces to the information realized by the intruder on attaining the f_{th} aim; Nfj – a set of numbers of the protection means which can potentially be used for counteracting the intruder's realization of the f_{th} aim at the j_{th} protection boundary (to neutralize the j_{th} menace being a part of the f_{th} aim) ($f = 1.2, \ldots, F$ $j = 1.2, \ldots, M$).

In this case, $B_f \subset A$, $\bigcup_{f=1}^{F} B_f = A$, $n_f = \left|B_f\right|$ и $\bigcup_{f=1}^{F}\bigcup_{j\in B_f,}^{n_f} N_j^f \subset D$.

Let us consider a system wherein the Markov casual process runs [1] under discrete conditions S_o, S_1,..., S_{nf}, S_{nf+1} ($f = 1,2,3, \ldots, F$). Each of the conditions S_j ($j = 1,2,\ldots, n_f$, $f = 1,2, \ldots F$) corresponds to realization by the intruder of only one menace from the set B_f ($f= 1,2, \ldots, F$). The condition S_o corresponds to the beginning of the intruder's work intended to realization of his aim (no one protection boundary is overcome); the condition S_j ($j = 1,2, \ldots, n_f - 1$) means realization of the j_{th} menace (overcoming of the j_{th} protection boundary); the condition Snf corresponds to realization by the intruder of the f_{th} aim; the condition Snf+1 means that the protection system has registered the intruder's touch and corresponding measures have been taken by the system or by guard.

In order to overcome the j_{th} boundary as the f_{th} aim is under realization ($j = 1,2, \ldots, n_f$, $f = 1,2, \ldots, F$) the intruder is able to use up to $k$fj attempts ($k$fj = $1,2,3, \ldots$) at most. While each of the attempts is under realization the system may get to the next condition (in this case the protection system does not register the intruder's actions), may remain in initial condition (that corresponds to unsuccessful realization of the given attempt) or may get to the $n_f + 1$ condition that corresponds to a normal reaction of the protection system to the intruder's actions. At the initial moment

$$P_o^f(0) = 1; P_j^f(0) = 0 (j = 1,2,...,n_f + 1; f = 1,2,...,F); x_{jm} = 0, \forall j,m; k_j^f = 1, \forall j, f,$$

where $X_{jn} = \{0.1\}$, $x_{jm} = 1$ if the m_{th} means is used at the j_{th} protection boundary, otherwise $x_{jm} = 0$, ($j \in B_f$, $j \neq 0$, $j \neq M + 1$; $m \in N$fj (l) is a probability for the system to be in the condition S_j at the l_{th} step.

In the case when transition probabilities are constant $p$fij $(l) = const$, (l = 1,2, …,K_f), we get the relationships to determine probabilities for the system to be in each of the conditions at the l_{th} step ($l = 1,2,\ldots,K_f$).

$$P_o^f(l) = P_0^f(l-1) p_{00}^f; \; P_j^f(l) = \sum_{\substack{i\in B_f, \\ i\neq M+1, \\ i\neq b_f^p}} P_i^f(l-1) p_{i,j}^f h_{ij}^f, \forall j \in B_f, j \neq 0,$$

where $h_{ij}^f = \begin{cases} g_j^f - в\ случае\ i \neq j \\ 1 - в\ случае\ i = j \end{cases}$,

K_f is the total number of the intruder's attempts to overcome the protection system; $g$fj is a probability of overcoming the j_{th} protection boundary at the intruder's attempt to attain the f_{th} aim $g_j^f = \left(1 - e^{-q_j \omega_f}\right) \prod_{m\in N_j^f} \left(1 - \rho_{jm}^f x_{jm}\right)$; $p$fjn is a probability of successful functioning of the m_{th} protection means at counteracting the intruder's actions at the j_{th} boundary as he tried to realize the f_{th} aim ($j \in B_f$, $j \neq 0$, $j \neq M + 1$; $f = 1,2, \ldots, F$; $m \in N$fj); q_1 is a coordination factor as the system gets to the j_{th} condition; ω_f is an average (maximum/minimum) level of the intruder's qualification as the f_{th} aim is under realization, $\omega_f \in [0.1]$ at the intruder's attempt to realize the f_{th} aim ($f = 1,\ldots,F$); $b$pf is an element of the B_f set corresponding to the condition Snf of the system.

In this case, the efficiency of the information protection system functioning can be determined with the help of the following parameters: an average value of losses in DTPS due to realization of all aims by the intruder; a

probability of realization of all aims by the intruder; a probability of a successful counteraction of the protection system to the intruder's actions intended to realization of all his aims; total cost of the protection system.
The values magnitudes can be determined from the following relationships.

1. An average body of all losses due to the intruder's actions as all his aims are attained and the total cost of the information protection system is, respectively,

$$C^p = \sum_{f=1}^{F} \sum_{l=1}^{K_f} \sum_{\substack{j \in B_f, \\ j \neq 0, \\ j \neq M+1}} P_j^f(l) c_{jf},$$

where $c_{jf} = c1\text{jf} + c2\text{jf} + c3\text{jf}$; $c1\text{jf}$, $c2\text{jf}$, $c3\text{jf}$ is the body of losses of the system due to infringement of the information confidentiality, the body of losses because some pieces of work were not implemented, the cost of the protection system recondiyioing in case the intrhder's j_{th} menace is realized at the attempt of attaining the f_{th} aim, respectively;
$C_{\text{jm}} = S0\text{m} + S1\text{jm}$ is the cost of the use of the m_{th} means at the j_{th} boundary; $S0\text{m}$ is the cost of the m_{th} means, $S1\text{jm}$ is the cost of the m_{th} means installation and maintenance at the j_{th} protection boundary.

2. The probability of realization of all the intruder's aims and the probability of a successful counteraction of the system to attaiming of all aims by the intruder is, respectively.

$$P^p = \prod_{f=1}^{F} \left(1 - \prod_{l=1}^{K_f} \left[1 - \sum_{\substack{j \in B_f, \\ j \neq b_f^p, \\ j \neq M+1}} P_j^f(l) p^f{}_{jb_f^p} h^f_{b_f^p} \right] \right)$$

REFERENCES:

1. E.S.Ventsel, L.A.Ovcharov, The Theory of Casual Processes and its Engineering Application. M: Nauka – 1991, 384 p.