УДК 519.816:004.056.53

МОДЕЛИРОВАНИЕ ДИНАМИКИ РЕАЛИЗАЦИИ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ НА ОСНОВЕ АППАРАТА СЕТЕЙ ПЕТРИ-МАРКОВА

Ю.К. Язов, А.П. Панфилов

Излагается методический подход к моделированию динамики реализации угроз несанкционированного доступа в компьютерных системах с использованием аппарата сетей Петри-Маркова

Наиболее полно учет основных факторов, влияющих на оценку возможности реализации угроз несанкционированного доступа (НСД) к информации в компьютерных системах (КС), можно провести, моделируя рассматриваемые процессы с использованием аппарата сетей Петри-Маркова, в основе которого лежат теории сетей Петри и полумарковских процессов [1-3].

Под сетью Петри-Маркова (СПМ) понимается множество $\Psi = \{\Pi, \mathrm{M}\}$, при этом Π - сеть Петри – двудольный граф вида:

$$\Pi = \{A, T, O_A(T), O_T(T)\}, \qquad (1)$$

где A - множество позиций сети Петри, моделирующих состояние рассматриваемого процесса;

T - множество переходов сети Петри, моделирующих условия перехода из состояния в состояние;

$O_A(T)$ - входная функция переходов (выходная функция позиций), отображающая множество A в множество T;

$O_T(A)$ - входная функция позиций (выходная функция переходов), отображающая множество T в множество A.

Параметрические особенности динамики реализации угроз отражаются множеством $\mathrm{M} = \{P, Q(t), \mathrm{Y}\}$, где P - вектор вероятностей, описывающих вероятность появления состояния процесса в начальный момент времени, $Q(t)$ - полумарковская матрица, характеризующая временные и стохастические параметры модели, Y - матрица логических условий, элементы которой равны:

$$\upsilon_{j(z),i(a)} = \begin{cases} L[s_{1(a),j(z)}, \ldots, s_{i(a),j(z)}, \ldots, s_{K(a),j(z)}], & \text{åñëè } a_{i(a)} \in O_A(z_{j(z)}); \\ 0, & \text{åñëè } a_{i(a)} \notin O_A(z_{j(z)}). \end{cases} \qquad (2)$$

В данном случае функция L - это логическая функция, разрешающая выполнение полушагов из переходов в состояния в соответствии со структурой сети Петри, где по-

The complete account of the main factors effecting the possibility estimation of unauthorized access threats realization to information in computer systems is possible to carry out, modelling the processes under review the use of Petri-Markovian mechanism based on the Petri net and semi-markovian process theories [1-3].

Petri-Markovian net (PMN) is regarded as $\Psi = \{\Pi, \mathrm{M}\}$, where Π is the Petri net - bipartite graph of :

$$\Pi = \{A, T, O_A(T), O_T(T)\}, \qquad (1)$$

where A is the set of Petri net positions modelling the status of the process;

T - is the set of Petri net transitions modelling the conditions of transition from state to state;

$O_A(T)$ is the transition input function (position output function), representing set A in set T;

$O_T(A)$ is the position input function (transition output function) representing set T into set A.

The parametric peculiarities of threat realization dynamics are presented by set $\mathrm{M} = \{P, Q(t), \mathrm{Y}\}$ where P - the probability vector depicting probability of process state occurrence at start time $Q(t)$ - the semi-markovian matrix characterizing the time and stochastic parameters of the model, Y - logical condition matrix, the elements of which are equal to:

$$\upsilon_{j(z),i(a)} = \begin{cases} L[s_{1(a),j(z)}, \ldots, s_{i(a),j(z)}, \ldots, s_{K(a),j(z)}], & \text{åñëè } a_{i(a)} \in O_A(z_{j(z)}); \\ 0, & \text{åñëè } a_{i(a)} \notin O_A(z_{j(z)}). \end{cases} \qquad (2)$$

In this case function L is the logical function allowing the carring out of half steps from transitions into states in accordance with the

лушаг от позиции с номером $i(a)$ к переходу с номером $j(z)$:

$$s_{i(a),j(z)} = (a_{i(a)}, z_{j(z)}),\ 1(a) \le i(a) \le K(a) \qquad (3)$$

определяет условия срабатывания перехода $z_{j(z)}$ в позицию $a_{j(a)} \in O_Z(a_{j(a)})$. Два последовательных полушага образуют шаг. Особенность такой сети, отличающая ее от обычной сети Петри, заключается в том, что каждый переход срабатывает только с определенной вероятностью.

Полумарковская матрица представляет собой произведение матрицы вероятностей переходов $\{p_{j(a)j(z)}\}$ и матрицы плотностей времени пребывания процесса в каждом j-м состоянии $\{f_{j(a)j(z)}(t)\}$, если считать, что переход происходит мгновенно, то есть:

$$Q(t) = \{p_{j(a)j(z)} \cdot f_{j(a)j(z)}(t)\}. \qquad (4)$$

Процесс реализации угрозы представляет собой последовательность перемещений, реализуемых в виде полушагов по СПМ. При этом СПМ пребывает в каждом состоянии некоторое случайное время, определенное соответствующей этому состоянию плотностью распределения, и затем выполняется полушаг и проверка логических условий переключения сети в следующее состояние. Последовательность состояний СПМ называется траекторией моделируемого процесса. Если сеть Петри является неконфликтной, то есть отсутствуют кратные выходные для переходов дуги, то аналитическое описание процесса в виде интегродифференциальных уравнений проводится достаточно просто по траекториям перемещений из начального состояния в конечное [4].

Пусть $h(tr : 1(a) \to j(a)) = h(tr_{1_j})$ - номер траектории из состояния $a_{1(a)}$ (здесь индекс с буквой (a), как и ранее, означает номер состояния) в состояние $a_{j(a)}$, которая содержит последовательность полушагов из состояния в переход, затем из перехода в состояние и т.д.:

$$s_{1[h(tr)]}, s_{2[h(tr)]}, \ldots, s_{i[h(tr)]}, \ldots, s_{j[h(tr)]}, \qquad (5)$$

Petri net structure where the half step from the position with number $i(a)$ to the transition with number $j(z)$,

$$s_{i(a),j(z)} = (a_{i(a)}, z_{j(z)}),\ 1(a) \le i(a) \le K(a) \qquad (3)$$

determines the actuation conditions of transition $z_{j(z)}$ in position $a_{j(a)} \in O_Z(a_{j(a)})$. Two consecutive half steps form a step. The peculiarity of such a net distinguishing it from common Petri net is that each transition operated only with a certain probability.

The semi-markovian matrix is a composition of transition probability matrix $\{p_{j(a)j(z)}\}$ and density matrix of process residence time in each j-state $\{f_{j(a)j(z)}(t)\}$ assuming the transition occurs immediately i.e.:

$$Q(t) = \{p_{j(a)j(z)} \cdot f_{j(a)j(z)}(t)\} \qquad (4)$$

The threat realization process represents the transfer sequence realized in the form of half steps on PMN. At that the PMN is resides in each state for some random time defined by the distribution density, corresponding to this state, and then the half step and check of logical conditions of net switching over to the next state are carried out.

The sequence of PMN conditions is called a modelled process trajectory. If Petri net is conflict-free, that is multiple outgoing for arche transitions are absent, then the analytical process description as the integro-differential equations is carried out simply enough on transfer trajectories from the initial to the finite state [4].

Let $h(tr : 1(a) \to j(a)) = h(tr_{1_j})$ - the number of trajectory from $a_{1(a)}$ state (here the index (a), as well as before, is a state number) into $a_{j(a)}$ state which contains the half step sequence from state to transition, then from transition to state, etc.:

$$s_{1[h(tr)]}, s_{2[h(tr)]}, \ldots, s_{i[h(tr)]}, \ldots, s_{j[h(tr)]}, \qquad (5)$$

where the second index each time corresponds either to the number of the state or to the number of the transition, included in the selected trajectory $h(tr)$. The number of such trajectories is equal to $H(tr)$.

The distribution probability and density of implementation time of the corresponding half step are defined as well as $p_{j(a)j(z)}$ and $f_{j(a)j(z)}$.

где второй индекс соответствует каждый раз или номеру состояния, или номеру перехода, входящих в выбранную траекторию $h(tr)$. Количество таких траекторий равно $H(tr)$.

Вероятность и плотность распределения времени выполнения соответствующего полушага определяются как $p_{j(a)j(z)}$ и $f_{j(a)j(z)}$. Тогда вероятность и плотность распределения времени перемещения из состояния $a_{1(a)}$ в состояние $a_{j(a)}$ по траектории $h(tr_{1j})$ определяется из соотношений:

$$p_{h(tr_{1j})} = \prod_{j[h(tr_{1j})]=1}^{J[h(tr_{1j})]} p_{j[h(tr_{1j})]}; \quad (6)$$

$$f_{h(tr_{1j})} = f_{1[h(tr_{1j})]} * f_{2[h(tr_{1j})]} * \ldots * f_{i[h(tr_{1j})]} * \ldots * f_{J[h(tr_{1j})]}, \quad (7)$$

где $J[h(tr_{1j})]$ - общее количество позиций и переходов в траектории $h(tr_{1j})$;

* - операция свертки,

а по всем возможным траекториям из соотношений:

$$p_{1(a)j(a)} = \prod_{h(tr_{1j})=1}^{H(tr_{1j})} p_{h(tr_{1j})}; \quad (8)$$

$$f_{1(a)j(a)} = \frac{\prod_{h(tr_{1j})=1}^{H(tr_{1j})} p_{h(tr_{1j})} \cdot f_{h(tr_{1j})}}{\prod_{h(tr_{1j})=1}^{H(tr_{1j})} p_{h(tr_{1j})}}. \quad (9)$$

Вид логической функции проще всего рассмотреть на конкретном примере. Пусть рассматривается и моделируется с помощью СПМ атака типа "Анализ сетевого трафика". Вид сети Петри для такой атаки показан на рис. 1.

Элементы матрицы, определяющие логические функции срабатывания сети, могут быть записаны (без учета направленности дуг графа) следующим образом:

$v_{1(a)5(a)} =$

	1(z)	2(z)	3(z)	4(z)	5(z)
1(a)	1	0	0	1	0
2(a)	0	1	0	0	0
3(a)	1	0	1	0	1
4(a)	0	1	1	0	0
5(a)	0	0	(3(a),3(z)∩(4(a),3(z)))	0	0

(10)

Then the probability and density transfer time distribution from state $a_{1(a)}$ into the state $a_{j(a)}$ on trajectory $h(tr_{1j})$ is found from the ratio:

$$p_{h(tr_{1j})} = \prod_{j[h(tr_{1j})]=1}^{J[h(tr_{1j})]} p_{j[h(tr_{1j})]}; \quad (6)$$

$$f_{h(tr_{1j})} = f_{1[h(tr_{1j})]} * f_{2[h(tr_{1j})]} * \ldots * f_{i[h(tr_{1j})]} * \ldots * f_{J[h(tr_{1j})]}, \quad (7)$$

where $J[h(tr_{1j})]$ is the total amount of positions and transitions in a trajectory $h(tr_{1j})$;

* - compression operation,

and on all possible trajectories from the ratio:

$$p_{1(a)j(a)} = \prod_{h(tr_{1j})=1}^{H(tr_{1j})} p_{h(tr_{1j})}; \quad (8)$$

$$f_{1(a)j(a)} = \frac{\prod_{h(tr_{1j})=1}^{H(tr_{1j})} p_{h(tr_{1j})} \cdot f_{h(tr_{1j})}}{\prod_{h(tr_{1j})=1}^{H(tr_{1j})} p_{h(tr_{1j})}}. \quad (9)$$

The easiest way to consider the logical function type is a concrete example.

Let's consider and model the attack of "the network traffic analysis" type with the help of PMN. The Petri net type for such an attack is shown on figure 1.

The matrix elements determining logical functions of net operation, can be written down (without taking into account graph arch directivity) in the following way:

$v_{1(a)5(a)} =$

	1(z)	2(z)	3(z)	4(z)	5(z)
1(a)	1	0	0	1	0
2(a)	0	1	0	0	0
3(a)	1	0	1	0	1
4(a)	0	1	1	0	0
5(a)	0	0	(3(a),3(z)∩(4(a),3(z)))	0	0

(10)

Here half step $3(z) \to 5(a)$ can be implemented only in case of half step $3(a) \to 3(z)$ and half step $4(a) \to 3(z)$ implementation, and symbol $\cap$ denotes "and" operation, one means "true", and zero is the absence of a half step.

Здесь полушаг $3(z) \to 5(a)$ может быть выполнен только в случае выполнения полушагов $3(a) \to 3(z)$ и $4(a) \to 3(z)$, знак $\cap$ означает операцию "и", единица означает

значение, равное "истина", а ноль – отсутствие полушага.

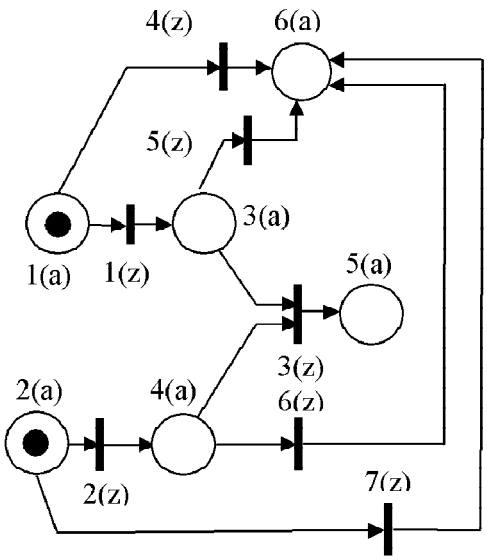

Рис. 1. Сеть Петри, моделирующая атаку типа "Анализ сетевого трафика" при отсутствии мер защиты: 1(a) – атакуемый хост включился в сеть общего пользования; 2(a) – хост злоумышленника включился в сеть общего пользования; 3(a) – атакуемый хост установил TCP-соединение с абонентом и начал обмен данными (наличие трафика хоста с абонентом); 4(a) – злоумышленник получил доступ к серверу (хосту), через который проходит трафик атакуемого хоста; 5(a) – злоумышленник получил имя пользователя и пароль; 6(a) – атака сорвана; 1(z) – установление TCP-соединения между хостом и абонентом; 2(z) – получение злоумышленником доступа к серверу, через который проходит трафик атакуемого хоста; 3(z) – анализ трафика (перехват пакетов атакуемого хоста); 4(z), 5(z), 6(z) и 7(z) – срыв атаки.

Поскольку полушаг из перехода в позицию (например, $3(z) \to 5(a)$) срабатывает мгновенно, то динамика срабатывания СПМ определяется только вероятностями срабатывания СПМ (перемещения из состояния в переход) и плотностями распределения времени нахождения процесса в каждом состоянии. Тогда в данном примере достаточно рассмотреть процесс перехода СПМ по двум траекториям из состояний $1(a)$ и $2(a)$ в переход $3(z)$.

Для первой из указанных траекторий имеет место следующая система интегро-дифференциальных уравнений:

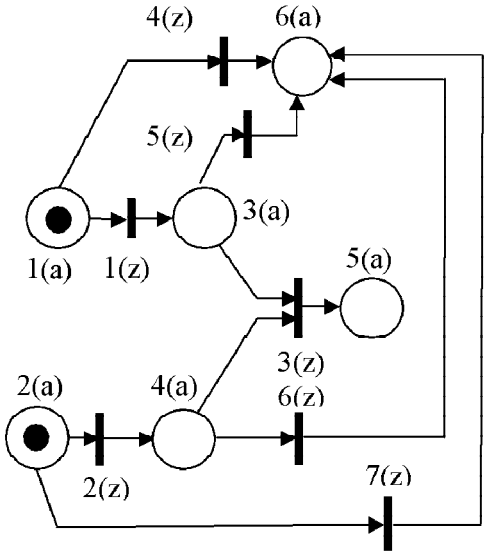

Fig. 1. Petri net modelling an attack of "network traffic analysis" with protective measures being absent: 1(a) - the attacked host cut in the public network; 2(a) - the attacker's host cut in the public network; 3(a) - the attacked host set the TCP-connection with the customer and begin data communication (host traffic with the customer is available); 4(a) - the attacker accessed the server (host) which the attacked host traffic passes throught; 5(a) - the attacker acquired user's name and password; 6(a) - the attack is upset; 1(z) - the TCP-connection is established between the host and the consumer; 2(z) - the attacker accessing to the server through which the attacked host traffic passes; 3(z) - traffic analysis (interception of the attacked host packages); 4(z), 5(z), 6(z) and 7(z) - the attack breakdown.

Since half step from transition to position (e.g., $3(z) \to 5(a)$) operates immediately, than PMN actuation dynamics is determined only by PMN actuation probabilities (transfer from state to transition) and the distribution densities of process residence time in each state.

In this example it is sufficient to consider the PMN transition process by two trajectories from states $1(a)$ and $2(a)$ to transition $3(z)$.

For the first trajectory the following system of integro-differential equations is used:

$$\Phi_{1(a)3(z)}(t) = \pi_{1(a)1(z)} \cdot \int_0^t f_{1(a)1(z)}(\tau) \cdot \Phi_{3(a)3(z)}(t-\tau) d\tau;$$

$$\Phi_{3(a)3(z)}(t) = \pi_{3(a)3(z)} \cdot \int_0^t f_{3(a)3(z)}(\tau)\, d\tau,$$

where $\pi_{1(a)1(z)}$ is the probability of TCP-connection establishment between the attacked host and the customer;

$$\Phi_{1(a)3(z)}(t) = \pi_{1(a)1(z)} \cdot \int_0^t f_{1(a)1(z)}(\tau) \cdot \Phi_{3(a)3(z)}(t-\tau) d\tau;$$

$$\Phi_{3(a)3(z)}(t) = \pi_{3(a)3(z)} \cdot \int_0^t f_{3(a)3(z)}(\tau) d\tau, \quad (11)$$

где $\pi_{1(a)1(z)}$ - вероятность установления атакуемым хостом TCP-соединения с абонентом;

$\pi_{3(a)3(z)}$ - вероятность наличия трафика между атакуемым хостом и абонентом.

Аналогично для второй из указанных траекторий имеет место следующая система интегродифференциальных уравнений:

$$\Phi_{2(a)3(z)}(t) = \pi_{2(a)2(z)} \cdot \int_0^t f_{2(a)2(z)}(\tau) \cdot \Phi_{4(a)3(z)}(t-\tau) d\tau;$$

$$\Phi_{4(a)3(z)}(t) = \pi_{4(a)3(z)} \cdot \int_0^t f_{4(a)3(z)}(\tau) d\tau, \quad (12)$$

где $\pi_{2(a)2(z)}$ - вероятность получения доступа злоумышленника в сеть, через который проходит трафик атакуемого хоста;

$\pi_{4(a)3(z)}$ - вероятность попыток получения злоумышленником прав пользователя атакуемого хоста.

Вероятность перехода СПМ из начального в конечное состояние определяется как вероятность того, что ко времени t перемещение пройдет по обеим траекториям:

$$P_u(t) = \Phi_{1(a)3(z)}(t) \cdot \Phi_{2(a)3(z)}(t). \quad (13)$$

Пусть плотности распределения вероятностей имеют вид:

$$f_{1(a)1(z)} = \lambda_1 \cdot e^{-\lambda_1 \cdot t}; \; f_{3(a)3(z)} = \lambda_3 \cdot e^{-\lambda_3 \cdot t};$$

$$f_{2(a)2(z)} = \lambda_2 \cdot e^{-\lambda_2 \cdot t}; \; f_{4(a)3(z)} = \lambda_4 \cdot e^{-\lambda_4 \cdot t},$$

где λ_1 - интенсивность TCP-соединения с абонентом атакуемого хоста;

λ_3 - интенсивность передачи сообщений абоненту атакуемым хостом;

λ_2 - интенсивность получения злоумышленником доступа к сегменту сети, через который проходит трафик атакуемого хоста;

λ_4 - интенсивность перехвата сообщений атакуемого хоста злоумышленником.

$\pi_{3(a)3(z)}$ - is the probability of traffic presence between the attacked host and the customer.

The following system of integro-differential equations is analogous for the second trajectory:

$$\Phi_{2(a)3(z)}(t) = \pi_{2(a)2(z)} \cdot \int_0^t f_{2(a)2(z)}(\tau) \cdot \Phi_{4(a)3(z)}(t-\tau) d\tau;$$

$$\Phi_{4(a)3(z)}(t) = \pi_{4(a)3(z)} \cdot \int_0^t f_{4(a)3(z)}(\tau) d\tau, \quad (12)$$

where $\pi_{2(a)2(z)}$ - the probability of the attacker accessing to the network which the attacked host traffic passes through;

$\pi_{4(a)3(z)}$ - the probability of the attacker's attempts to acquire the user rights of the attacked host.

The probability of PMN transition from the initial to finite state is defined as the probability of the fact that by time t the transition will pass by both trajectories:

$$P_u(t) = \Phi_{1(a)3(z)}(t) \cdot \Phi_{2(a)3(z)}(t). \quad (13)$$

Let the probability distribution density have the following form:

$$f_{1(a)1(z)} = \lambda_1 \cdot e^{-\lambda_1 \cdot t}; \; f_{3(a)3(z)} = \lambda_3 \cdot e^{-\lambda_3 \cdot t};$$

$$f_{2(a)2(z)} = \lambda_2 \cdot e^{-\lambda_2 \cdot t}; \; f_{4(a)3(z)} = \lambda_4 \cdot e^{-\lambda_4 \cdot t}$$

where λ_1 - the intensity of TCP-connection with the attacked host consumer;

λ_3 - the intensity of message transfer to the consumer by the attacked host;

λ_2 - the intensity of attacker's accessing to the network segment through which the attacked host traffic passes.

λ_4 - the intensity of interception of attacked host messages by the attacker.

Then:

$$\Phi_{1(a)3(z)} = L^{-1}\{\pi_{1(a)1(z)} \cdot \pi_{3(a)3(z)} \frac{\lambda_1 \cdot \lambda_3}{s \cdot (s+\lambda_1) \cdot (s+\lambda_3)}\} \text{ and}$$

$$\Phi_{2(a)3(z)}(t) = L^{-1}\{\pi_{2(a)2(z)} \pi_{4(a)3(z)} \cdot \frac{\lambda_2 \cdot \lambda_4}{s \cdot (s+\lambda_2) \cdot (s+\lambda_4)}\} \quad (14)$$

Where L^{-1} - is the Laplas inversion with parameter s, or taking the inversion we get:

$$\Phi_{1(a)3(z)}(t) = \pi_{1(a)1(z)} \cdot \pi_{3(a)3(z)} \cdot$$

$$\cdot [1 + \frac{\lambda_1}{\lambda_3 - \lambda_1} \cdot e^{-\lambda_3 \cdot t} - \frac{\lambda_3}{\lambda_3 - \lambda_1} \cdot e^{-\lambda_1 \cdot t}]; \quad (15)$$

Тогда:

$$\Phi_{1(a)3(z)} = L^{-1}\{\pi_{1(a)1(z)} \cdot \pi_{3(a)3(z)} \frac{\lambda_1 \cdot \lambda_3}{s \cdot (s+\lambda_1) \cdot (s+\lambda_3)}\} \text{ и}$$

$$\Phi_{2(a)3(z)}(t) = L^{-1}\{\pi_{2(a)2(z)}\pi_{4(a)3(z)} \cdot \frac{\lambda_2 \cdot \lambda_4}{s \cdot (s+\lambda_2) \cdot (s+\lambda_4)}\} \quad (14)$$

где L^{-1}- обратное преобразование Лапласа с параметром s ,или, беря обратное преобразование, получаем:

$$\Phi_{1(a)3(z)}(t) = \pi_{1(a)1(z)} \cdot \pi_{3(a)3(z)} \cdot$$

$$\cdot [1 + \frac{\lambda_1}{\lambda_3 - \lambda_1} \cdot e^{-\lambda_3 \cdot t} - \frac{\lambda_3}{\lambda_3 - \lambda_1} \cdot e^{-\lambda_1 \cdot t}]; \quad (15)$$

$$\Phi_{2(a)3(z)}(t) = \pi_{2(a)2(z)} \cdot \pi_{4(a)3(z)} \cdot$$

$$\cdot [1 - \frac{\lambda_4}{\lambda_4 - \lambda_2} \cdot e^{-\lambda_2 \cdot t} + \frac{\lambda_2}{\lambda_4 - \lambda_2} \cdot e^{-\lambda_4 \cdot t}]. \quad (16)$$

Если $\lambda_2 = \lambda_4$, то формула (16) имеет вид:

$$\Phi_{2(a)3(z)}(t) = \pi_{4(a)3(z)} \cdot \pi_{2(a)2(z)} \cdot [1 - (1 + \lambda_2 \cdot t) \cdot e^{-\lambda_2 \cdot t}]$$

При этом формула для расчета вероятности реализации атаки "Анализ сетевого трафика " имеет вид

$$P_u(t) = \pi_{1(a)1(z)}\pi_{3(a)3(z)}\pi_{4(a)3(z)}\pi_{2(a)2(z)} \cdot$$

$$\cdot [1 - \frac{\lambda_3}{\lambda_3 - \lambda_1} \cdot e^{-\lambda_1 \cdot t} + \frac{\lambda_1}{\lambda_3 - \lambda_1} \cdot e^{-\lambda_3 \cdot t}] \cdot [1 - \frac{\lambda_4}{\lambda_4 - \lambda_2} \cdot e^{-\lambda_2 \cdot t} + \frac{\lambda_2}{\lambda_4 - \lambda_2} \cdot e^{-\lambda_4 \cdot t}] \quad (17)$$

Характерным в данном случае является то, что вложенная цепь Маркова является приводимой [2], при этом вероятность перехода полумарковского процесса в конечное состояние не превышает произведения вероятностей переходов цепи Маркова из состояния в состояние. График полученной зависимости приведен на рис. 2, где положено $\pi = \pi_{1(a)1(z)} \cdot \pi_{3(a)3(z)} \cdot \pi_{4(a)4(z)} \cdot \pi_{2(a)2(z)}$.

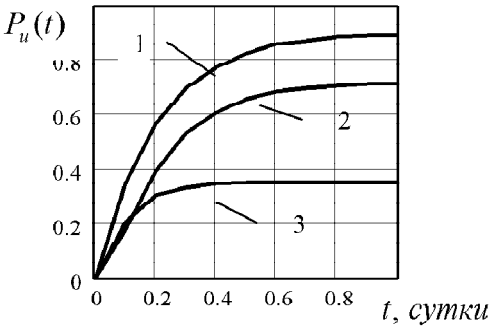

Рис. 2. Зависимость от времени вероятности реализации угрозы атаки типа "Анализ сетевого трафика" при отсутствии мер защиты

$$\Phi_{2(a)3(z)}(t) = \pi_{2(a)2(z)} \cdot \pi_{4(a)3(z)} \cdot$$

$$\cdot [1 - \frac{\lambda_4}{\lambda_4 - \lambda_2} \cdot e^{-\lambda_2 \cdot t} + \frac{\lambda_2}{\lambda_4 - \lambda_2} \cdot e^{-\lambda_4 \cdot t}] \quad (16)$$

If $\lambda_2 = \lambda_4$, then equation (16) has the form:

$$\Phi_{1(a)3(z)}(t) = \pi_{4(a)3(z)} \cdot \pi_{2(a)2(z)} \cdot [1 - (1 + \lambda_2 \cdot t) \cdot e^{-\lambda_2 \cdot t}]$$

So the probability calculation formula of "network traffic analysis" attack realization has the following form:

$$P_u(t) = \pi_{1(a)1(z)}\pi_{3(a)3(z)}\pi_{4(a)3(z)}\pi_{2(a)2(z)} \cdot$$

$$\cdot [1 - \frac{\lambda_3}{\lambda_3 - \lambda_1} \cdot e^{-\lambda_1 \cdot t} + \frac{\lambda_1}{\lambda_3 - \lambda_1} \cdot e^{-\lambda_3 \cdot t}] \cdot [1 - \frac{\lambda_4}{\lambda_4 - \lambda_2} \cdot e^{-\lambda_2 \cdot t} + \frac{\lambda_2}{\lambda_4 - \lambda_2} \cdot e^{-\lambda_4 \cdot t}] \quad (17)$$

In this case it is characteristic that the imbedded Markov chain transition to the finite state doesn't exceed the probability composition of Markov chain transitions from state to state.

The graph of acquired dependence is given in fig. 2 where:

$$\pi = \pi_{1(a)1(z)} \cdot \pi_{3(a)3(z)} \cdot \pi_{4(a)4(z)} \cdot \pi_{2(a)2(z)} \cdot$$

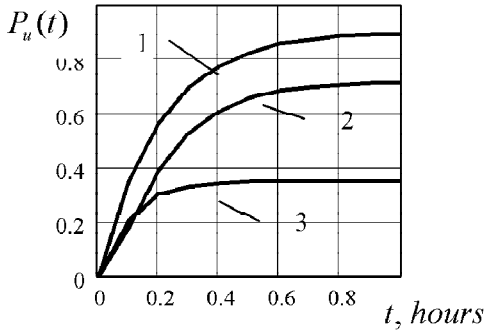

Fig. 2. Dependance on probability time of "network traffic analysis" attack threat realization in the absence of protection measures

1) $\lambda_1 = 5\frac{1}{hours}$, $\lambda_2 = 10\frac{1}{hours}$, $\lambda_3 = \lambda_4 = 720\frac{1}{hours}$, $\pi = 0.9$;

2) $\lambda_1 = 5\frac{1}{hours}$, $\lambda_2 = 10\frac{1}{hours}$, $\lambda_3 = \lambda_4 = 600\frac{1}{hours}$, $\pi = 0.7$;

3) $\lambda_1 = 10\frac{1}{hours}$, $\lambda_2 = 30\frac{1}{hours}$, $\lambda_3 = \lambda_4 = 360\frac{1}{hours}$, $\pi = 0.35$

The awkwardness of the conducted calculations impedes considerably the PMN mechanism use for modeling the processes under consideration.

1) $\lambda_1 = 5\frac{1}{сутки}, \lambda_2 = 10\frac{1}{сутки}, \lambda_3 = \lambda_4 = 720\frac{1}{сутки}, \pi = 0.9;$

2) $\lambda_1 = 5\frac{1}{сутки}, \lambda_2 = 10\frac{1}{сутки}, \lambda_3 = \lambda_4 = 600\frac{1}{сутки}, \pi = 0.7;$

3) $\lambda_1 = 10\frac{1}{сутки}, \lambda_2 = 30\frac{1}{сутки}, \lambda_3 = \lambda_4 = 360\frac{1}{сутки}, \pi = 0.35$

Громоздкость проводимых расчетов существенно затрудняет практическое применение аппарата сетей Петри-Маркова для моделирования рассматриваемых процессов.

Вместе с тем возможность математического моделирования параллельных процессов значительно повышает адекватность разрабатываемых моделей и, несомненно, способствует повышению качества оценки защищенности информации в КС от угроз НСД.

Литература

1. Котов, В.Е. Сети Петри/ В.Е. Котов. - М.: Наука. 1984. 160 с.

2. Сильвестров, Д.С. Полумарковские процессы с дискретным множеством состояний (основы расчета функциональных и надежностных характеристик стохастических систем)/ Д.С. Сильвестров. - М.: Советское радио. 1980. 272 с.

3. Тихонов, В.И. Марковские процессы / В.И. Тихонов, М.А. Миронов. - М.: Советское радио, 1977. 357 с.

4. Сабо, Ю.И. Применение сетей Петри с марковскими свойствами для анализа отказоустойчивости систем с резервированием / Ю.И Сабо // Известия вузов. Приборостроение. 2004. Т. 47. №12. С. 18-23.

At the same time the mathematic modeling possibility of parallel processes increases significantly the adequacy of the developed models and, undoubtedly, improves the estimation of information protectability from unauthorized access threats in computer systems.

Reference

1. V.E. Kotov Petri nets. - M.: the Science, 1984.-160 p.

2. D.S. Silverstov. Semimarkov processes with state discrete set (the basis of functional and reliability characteristics calculation of stochastic systems). - M.: Soviet radio, 1980. - 272 p.

3. V.I.Tihonov, M.A.Mironov. Markov processes. M.: Soviet radio, 1977. - 357 p.

4. J.I.Sabo. Use of Petri nets of Markov features for fault tolerance analysis of the systems with reservation. Proceedings of high schools. Instrument making industry. Vol. 47, №12, 2004. - p. 18-23.

Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю

State science research experimental institute of technical information protection problems of Federal service of technical and export control

DYNAMICS MODELLING OF THREAT REALIZATION OF UNAUTHORIZED ACCESS TO INFORMATION IN COMPUTER SYSTEMS BASED ON PETRI-MARKOVIAN NET MECHANISM

U.K. Yazov, A.P. Panfilov

The methodical approach to the dynamics modelling of threat realization of unauthorized access to information in computer systems the use of Petri-Markovian mechanism is described