MSC 68T05, 62J07, 68Q32 DOI: 10.14529/mmp210404

SIMULATION OF PROCESSES TO PROTECT INFORMATION OF INFORMATIZATION OBJECTS AGAINST LEAKAGE THROUGH TECHNICAL CHANNELS USING AN APPARATUS OF PETRI–MARKOV NETS

***O.S. Avsentiev*[1]*, A.O. Avsentiev*[1]*, A.G. Krugov*[2]*, Yu.K. Yazov*[3]**

[1]Institute of the Ministry of Internal Affairs, Voronezh, Russian Federation

[2]Directorate of private security of the National Guard troops in the Tver region, Russian Federation

[3]Voronezh State Technical University, Voronezh, Russian Federation

E-mails: osaos@mail.ru, aoaao8787@mail.ru, krtemik@gmail.com, yazoff_1946@mail.ru

We propose an approach to simulation of information protection processes at informatization objects in the dynamics of realizing threats of its leakage through technical channels using the apparatus of composite Petri–Markov nets. We investigate the interrelationships of the processes of transferring information at the object of informatization, its interception by a violator from outside this object through technical channels and protection against interception. Analytical expressions are obtained for calculating the probabilistic-temporal characteristics of simulated processes in order to assess the possibility of a violator implementing threats of information leakage at objects of informatization; protection of this information through the use of preventive measures aimed at blocking or anticipating the actions of the violator to implement these threats.

Keywords: technical channel of information leakage; protection of information; preventive measure of protection; protection efficiency; probabilistic-temporal characteristic; branching process; logical condition; process modelling; composite Petri–Markov net.

Abbreviations

CPMN – composite Petri–Markov net; IO – informatization object; IP – information process; IPn – information protection; PI – process of interception; RRT – rapid response team; SE – structural element; TCIL – technical channel of information leakage; TM – technical means; TMII – technical means of information interception.

Introduction

Modelling of processes to protect information of informatization objects (IO) and obtaining quantitative estimates of its security taking into account the dynamics of the implementation of threats of leakage of this information through technical channels is one of the important problems in the study of such processes. Failure to take into account the time factor characterizing the indicated dynamics leads to the fact that the assessment of information security turns out to be overestimated, since it is based only on identifying the frequency and energy conditions of its interception. Attempts to take into account the time factor by expert means lead to incorrect estimates, since experts are not able to cover the entire set of conditions and parameters that are essential for intercepting protected information in time.

The problem under consideration is further complicated by the fact that it is necessary to simulate heterogeneous, branched, partial processes carried out both sequentially and in parallel in the presence of different logical conditions for intercepting information through technical channels of information leakage (TCIL). In addition, in such models, it is necessary to take into account the impact on the security of information of various measures of its protection. However, to date, indicators, and even more so, algorithms for assessing such an impact, were not developed.

Therefore, there exists a contradiction, the practical side of which consists in the following two facts. On the one hand, when assessing the security of information on the IO against leakage through the TCIL, there is the need to take into account, along with the frequency and energy conditions of information interception, the time factor, which cannot be done expertly. On the other hand, there is the lack of mathematical models for such an assessment.

The theoretical side of the problem is as follows. The dynamics of the implementation of the processes under consideration is characterized by a random sequence of changes in their states in time. Taking into account the very limited possibilities of using simulation models for the analysis of such processes (based, for example, on the development of computer programs, the use of the apparatus of Petri nets [1–4]), the main attention is paid to the use of methods that allow to obtain analytical relations for calculating indicators of the possibility of performing simulated processes in time. In [5, 6], approaches based on Markov and semi-Markov processes are used for such simulation. However, it turned out that many of the processes of information interception to be modeled are characterized by ramification, the presence of actions performed parallel, and logical conditions that determine the possibility of performing certain actions. This fact excludes the direct use of the apparatus of Markov processes for modelling. At the same time, the introduction of various logical conditions significantly limits the use of the apparatus of semi-Markov processes. In this regard, a different approach to the analytical modelling of the processes of information interception through the TCIL in time is required. To this end, the most expedient is the use of the apparatus of Petri–Markov nets, which was previously used to quantitatively assess the effectiveness of information protection from unauthorized access in computer systems [7] and in information systems of electronic document management [8]. The possibilities to use this apparatus for modelling the processes of protection of information of IO against leakage through technical channels were not considered previously.

1. Models of Processes of Information Leakage Through Technical Channels in the Absence of Security Measures

The emergence of TCIL on the IO is due to the presence of, on the one hand, the information process (IP), during which the protected information is transmitted and/or received, and on the other hand, the process of interception (PI) of such information by the violator. The protected information may include speech (audio) containing information of limited distribution, text, video and graphic information, as well as data on computer networks of IO and their elements (type of operating systems, equipment, etc.).

The TCIL includes:
a set of technical means (TM) that play the role of a source of information, and structural elements (SE) that make up the channel-forming environment;
the physical medium through which the interception of information can be carried out by the violator (radio emission, optical medium, acoustic medium, etc. [9–12]);
technical means of information interception (TMII) of the violator (radio receivers of interception, directional microphones, stethoscopes, acoustic bookmarks, laser acoustic location systems, etc. [13–18]).

The possibility to intercept information through the TCIL is determined not only by the functional and technical characteristics of the indicated constituent elements of the TCIL, but also by the dynamics of the IP and PI implementation. This is due to the fact that, firstly, during the IP, the transmission (reception) of information is carried out, as a rule, episodically at random times not known to the violator. Second, a TMII can:
1) constantly be within the zone of possible interception of the information necessary to the violator (at a distance at which the energy conditions of interception are fulfilled), for example, in a building adjacent to the IO or in the form of a sensor secretly installed on the IO itself. In this case, the dynamics of information interception is determined only by the dynamics of transmission of messages to IO containing protected information;
2) occasionally appear within the zone of possible interception of information and stay there for a limited time. In this case, the dynamics of information interception is determined not only by the dynamics of message transmission to the IO, but also by the dynamics of the emergence and functioning of the TMII.

All this makes it necessary to take into account not only the presence of energy conditions of interception, but also the possibility of intercepting in time, when assessing the possibility of intercepting the protected information through the TCIL. This assessment can be based on the theory of event streams [19].

Consider *the first of the two indicated situations* of information interception in the absence of security measures. As an indicator of the possibilities of interception under these conditions, it is advisable to use, by analogy with [19], the probability $P_i^{(0)}(t)$ that the messages containing confidential information are intercepted through the i-th TCIL for a given time, which is calculated as follows.

Let the total intensity of message transmission to the IO be $\overline{\mu_{io}}$ on average, while the probability that the message contains confidential information is p_{io} on average. Then, under the condition that the measures of information protection (IPn) are absent, the probability of intercepting at least one such message with an exponential approximation is calculated by the formula:

$$P_{i,\geq 1}^{(0)}(t) = 1 - exp\left(-\overline{\mu_{io}} \cdot p_{io} \cdot t\right). \tag{1}$$

In [19], the validity of such an approximation is shown already for $p_{io} < 0,4$. With an increase in p_{io}, the probability of interception of messages quickly approaches to 1 and it remains only to state the fact of interception. If it is necessary to evaluate the possibility of intercepting N messages through the i -th TCIL, then formula (1) is transformed to the form:

$$P_{i,N}^{(0)}(t) = 1 - \left[1 - \gamma\left(\overline{\mu_{io}} \cdot p_{io} \cdot t, N\right)\right] \approx 1 - \sum_{n=0}^{N-1} \left(\overline{\mu_{io}} \cdot p_{io} \cdot t\right)^n \cdot \exp\left(-\overline{\mu_{io}} \cdot p_{io} \cdot t\right), \tag{2}$$

where $\gamma(a, b)$ is an incomplete gamma function with the parameters a and b.

If the total number of TCILs is I, then the probability of interception through at least one of the channels is calculated as follows:

$$P_{I,\geq 1}^{(0)}\left(t\right) = 1 - \prod_{i=1}^{I}\left[1 - P_{i,\geq 1}^{(0)}\left(t\right)\right] \text{ – for at least one message;} \tag{3}$$

$$P_{I,N}^{(0)}\left(t\right) = 1 - \prod_{i=1}^{I}\left[1 - P_{i,N}^{(0)}\left(t\right)\right] \text{ – for } N \text{ messages.} \tag{4}$$

Consider *the second of the two indicated situations* of information interception. Let the flow of events corresponding to the appearance of a TMII within the zone of possible interception of information be described by the average intensity $\overline{\mu_{\text{tmii}}}$ and the average duration $\overline{\tau_{\text{tmii}}}$, and suppose that the flow of events corresponding to the transmission of messages containing confidential information to the IO is described by the average intensity $\overline{\mu_{io}}$ and the average duration of such transmission $\overline{\tau_{io}}$. Then the possibility of intercepting at least one message in the absence of protection measures is determined by the probability of the coincidence of these flows [19]:

$$P_{\geq 1}^{(0)}\left(t\right) = 1 - exp\left[-\overline{\mu_{io}} \cdot \overline{\mu_{\text{tmii}}} \cdot \left(\overline{\tau_{io}} + \overline{\tau_{\text{tmii}}}\right) \cdot p_{io} \cdot t\right] \tag{5}$$

If it is necessary to estimate the possibility of intercepting exactly N messages, then the probability $P_N^{(0)}(t)$ is calculated by formula (2), where the intensity of the coincidence flow $\overline{\mu_{io}} \cdot \overline{\mu_{\text{tmii}}} \cdot (\overline{\tau_{io}} + \overline{\tau_{\text{tmii}}})$ is used instead of the intensity $\overline{\mu_{io}}$. If there are I channels, then relations similar to (3) and (4) are used to estimate the possibility of leakage through at least one of the channels.

2. Models of Processes of Information Leakage Through Technical Channels Under Conditions of Application of Protection Measures

The dynamics of the information interception through TCIL can be significantly influenced by the application of adequate protection measures, which can be organizational and technical. The protection measures can be preventive, that is, they can be applied preliminarily at the stage of development of the IO, for example, by soundproofing the premises, shielding and grounding the screens of the TM of IO, etc., or the protection measures can be used during the preparation and holding of events (for example, holding meetings, conferences, gatherings, etc.) by searching for and expelling (or arresting) the violator from the territory of the object or from the adjacent territory, searching and eliminating stowing devices, setting acoustic and electromagnetic interference by special rapid response teams (RRT) from the IO security service [14].

If *the measure is preventive* and when applied, the corresponding i-th TCIL is not eliminated with the probability $1 - p_{det}^{(i)}$, where $p_{det}^{(i)}$ is the probability of detecting the i-th TCIL, the possibility to intercept information is determined, firstly, by the probability that the channel is not eliminated, and secondly, by the time characteristics of the transmission of messages to the IO containing information of limited access. Taking into account relation (1), under the condition of using measures of information protection, the probability of intercepting at least one message through the i-th channel in the course of the event during the time t is calculated by the formula:

$$P_{i,\geq 1}^{(\text{IPn})}\left(t\right) = \left(1 - p_{det}^{(i)}\right)\left[1 - exp\left(-\overline{\mu_{io}} \cdot p_{io} \cdot t\right)\right]. \tag{6}$$

If there are I channels of leakage, then the probability of intercepting the same information through at least one of the channels is determined as follows:

$$P_{I,\geq 1}^{(\mathrm{IPn})}(t) = \left(1 - \prod_{i=1}^{I} p_{det}^{(i)}\right)\left[1 - exp\left(-\overline{\mu_{io}} \cdot p_{io} \cdot t\right)\right]. \tag{7}$$

In the case of assessing the possibility of information leakage when applying protection measures in *the course of an event*, it is necessary to take into account the probabilistic and temporal characteristics of the application processes and the relationship of these measures with each other. In order to take into account such a relationship, logical conditions are introduced that determine the procedure for applying a set of protection measures. For modelling such processes, the apparatus of composite Petri–Markov nets (CPMN) [19] is most suitable, the possibility of using which for modelling processes of information leakage through TCIL was not previously considered.

3. Brief Description of Apparatus of Composite Petri–Markov Nets

The CPMN is a set of several subprocesses (partial processes) connected with each other by logical transitions. As well as the traditional Petri–Markov nets, the CPMNs proposed in [20] are represented in the form of directed graphs, where the vertices correspond to states (circles) the lines indicate the transitions of the process from state to state, and the arcs indicate the directions of the transitions. At the same time, in the CPMN, transitions can be simple and logical, that is, there is response of a transition under the certain logical conditions, such as “AND”, “OR”, “AND-NOT”, “OR-NOT”, “AND-OR” and others, which often take place when modelling the processes of implementing threats to information security.

If there is no branching in a partial process when the process leaves any position in transitions, then the apparatus of Markov processes is used for modelling. Fig. 1 presents an example of a fragment of a graph of CPMN constructed using partial Markov processes with logical conditions.

If the exit from the position forks, then the apparatus of semi-Markov processes is used. The sequence of movements along the CPMN is realized in the form of half-steps, while a half-step from position to transition occurs in a finite random time, and a half-step from transition to position occurs instantly. To indicate the movement of the process along the CPMN, chips (markers) are used, as in Petri nets.

Regardless of the form of the distribution functions of the time terms, the mathematical expectation of the total movement time is calculated by the formula

$$\overline{\tau_{\Sigma}^{(r)}} = \sum_{n=1}^{N^{(r)}} \overline{\tau_{n-1,n}^{(r)}} \tag{8}$$

where $\overline{\tau_{n-1,n}}$ are the mathematical expectations of the time terms, $n = \overline{1, N^{(r)}}$.

The total time of the CPMN response is determined by the times of execution of partial processes and the times of response of logical transitions. If the partial process is semi-Markov, that is, there are alternative scenarios, each of which can be chosen with a certain probability (Fig. 2), then the execution time of the partial process is determined in the same way as for the Markov process, and the probability of the execution of the

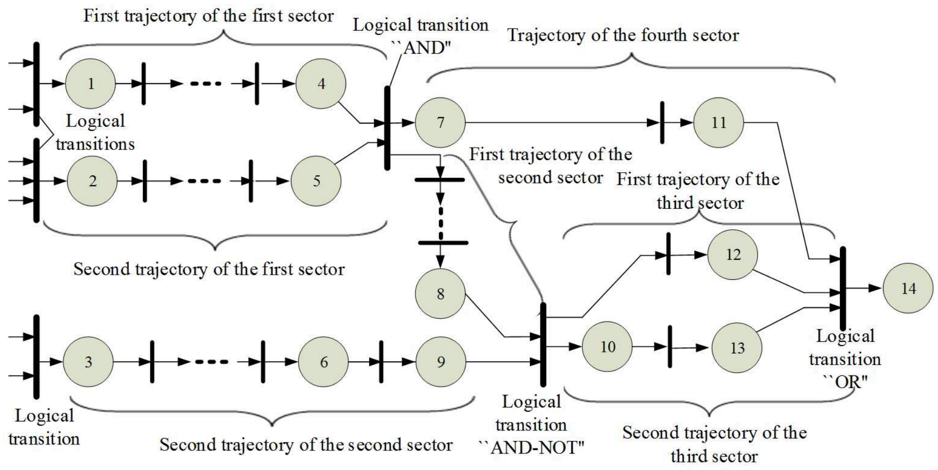
First trajectory of the first sector
Logical transition "AND"
Trajectory of the fourth sector
Logical transitions
First trajectory of the second sector
First trajectory of the third sector
Second trajectory of the first sector
Logical transition "OR"
Logical transition
Second trajectory of the second sector
Logical transition "AND-NOT"
Second trajectory of the third sector
1
2
3
4
5
6
7
8
9
10
11
12
13
14

Fig. 1. An example of a fragment of a graph of a composite Petri–Markov net constructed using partial Markov processes

embedded Markov chain is the product of the probabilities of the choice of options, leading the partial process to the second logical transition

$$\pi_{0,N} = \pi_{1,2} \cdot \pi_{2,m+1}. \tag{9}$$

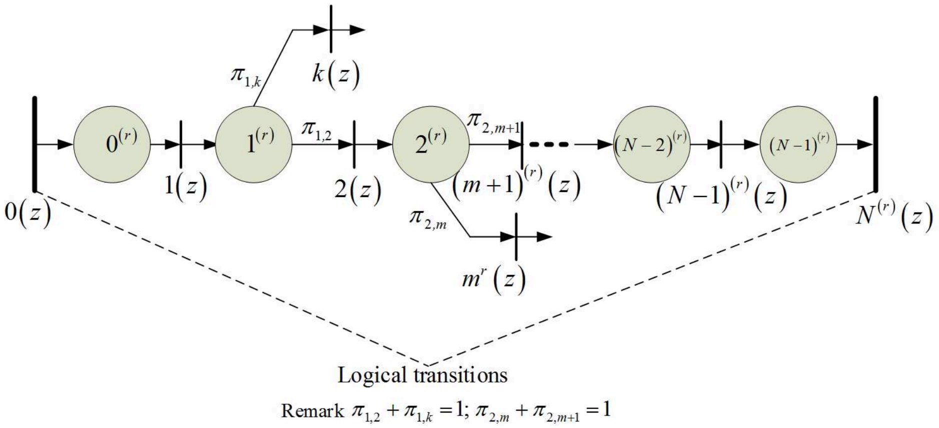

Fig. 2. Trajectory of a process moving along a Petri–Markov net between two logical transitions in a semi-Markov partial process

In this case, the probability that the partial process reaches the logical transition $N^{(r)}(z)$ is calculated as follows:

$$P_{0,N^{(r)}}(t) = \pi_{1,2} \cdot \pi_{2,m+1} \cdot \int_0^t [f_{0,1}(t) * f_{1,2}(t) * ... * f_{N-1,N}(t)]\, dt, \tag{10}$$

where * is a convolution operation that is sequentially performed for a pair of distribution densities, for example,

$$f_{0,1}(t) * f_{1,2}(t) = \int_0^\infty f_{0,1}(x-y) \cdot f_{1,2}(y) dy. \tag{11}$$

With an exponential approximation, the calculation is greatly simplified, since

$$f_{\Sigma}(t) = \frac{1}{\overline{\tau_{\Sigma}}} \cdot \exp\left(-\frac{t}{\overline{\tau_{\Sigma}}}\right), \tag{12}$$

and $\overline{\tau_{\Sigma}}$ is calculated by formula (8).

Let us consider the application of the described apparatus for assessing the possibilities of realizing the threats of information leakage through TCIL under the conditions of the application of protective measures during the events at the IO.

4. Mathematical Models of Processes of Realization of Information Leakage Threats

The process of realization of a threat of the information leakage through the TCIL during the event is determined both by the fulfillment of the energy conditions for detecting signals containing protected (intercepted by the violator) information in a particular physical field, and by a number of temporal characteristics concerning the violator's actions, preparation and conduct of an event at the IO, during which information can be intercepted through TCIL, the application of adequate protective measures. Considering the possible actions of a violator, note that the actions can be variant and, as a rule, are random in time. Therefore, a violator can appear on the territory adjacent to the IO either before the start of the event (option "a"), or after its start (option "b"). If $\overline{t_{sp}}$ and $\overline{t_{tool}}$ are estimates of average time between beginning of the workday and start of the event and the average time of arrival of the violator on the territory, respectively, then we can calculate the probabilities of the arrival of the violator before the start of the event π_a and after its start π_b as follows:

$$\pi_a = \overline{t_{sp}} \big/ \left(\overline{t_{sp}} + \overline{t_{tool}}\right) \text{ and } \pi_b = \overline{t_{tool}} \big/ \overline{t_{sp}} + \overline{t_{tool}} \tag{13}$$

Arriving on the territory, the violator chooses a place to implement the interception of information, deploys and configures the TMII, initiates stowage devices, if the devices are installed, and starts interception if the event is conducted already, or waits for the start of the event and then intercepts. At the same time, the violator examines the territory in order to detect the RRT. If the RRT is detected by the violator, then he either stops intercepting and leaves the territory, or ignores the appearance of the RRT and hides the TMII only when RRT approaches [14].

The dynamics of actions at the IO is characterized by temporal characteristics connected with, firstly, the preparation and conduct of the event, and secondly, the application of protective measures. The influence of protective measures on the possibility of suppressing the TCIL is assessed by indicators, which, as a rule, are the corresponding probabilities (detection and expulsion from the territory of the violator by the RRT within a given time, suppression of the TMII by interference excluding or significantly reducing the possibility of intercepting information). To calculate such indicators, it is necessary to have appropriate models. As an example, we consider such a model for the process of interception of speech information by a violator through an acoustic channel under the following conditions:

the use of the RRT to identify and expel the violator, search and eliminate stowing devices that can be installed in advance. The elimination of stowing devices leads to the impossibility of information interception by the violator;

setting acoustic interference using an appropriate generator, if the RRT detects neither the violator nor the stowing devices. In this case, the interception of information is either possible with a low probability, or completely blocked. The elimination of stowing devices does not exclude the possibility that the violator intercept speech information using a directional microphone, however, the expulsion of the violator from the territory makes it completely impossible to intercept the information.

Fig. 3 presents the graph of the CPMN that simulates the change in the state of the process of intercepting speech information through the acoustic channel under the conditions of applying the considered protection measures, from its beginning to the state when conditions for interception are formed. In this case, it is assumed that there are two possible situations in which the modeled process can come.

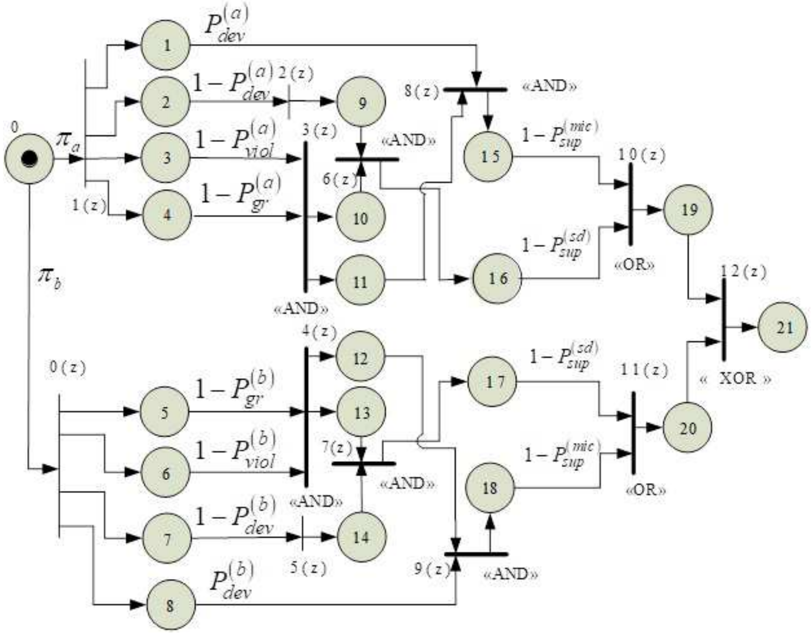

Fig. 3. Graph of a composite Petri–Markov net modelling the process of speech information leakage through the acoustic channel

The first situation corresponds to the case when the RRT was unable to locate and eliminate the indicated devices. *The second situation* corresponds to the case when the stowage devices were found and eliminated before the beginning of the interception.

In Fig. 3, the numbers without the letter z denote the positions corresponding to the states of the process, and the numbers with the letter z denote the transitions, while the bold lines indicate the logical transitions corresponding to the logic “AND” when the markers approach the transition along all incoming arcs, and the logic “XOR” (an exclusive choice) when only one of the options “a” or “b” is selected with a given probability (π_a or π_b).

0 stands for the initial state of the process: the violator is ready to go to the IO, preparation for the event begins in the IO;

1, 2 and 7, 8 stand for beginning of the search by the RRT for stowing devices in options “a” and “b”, respectively;

3 and 6 stand for beginning of the search by the RRT for the violator in the territory in options “a” and “b”, respectively;

4 and 5 stand for the fact that the violator, after arriving on the territory, begin to inspect it in order to detect the RRT in options “a” and “b”, respectively;

9 and 14 stand for the fact that the RRT did not find stowing devices with the probability $1 - P_{dev}^{(a)}$ and $1 - P_{dev}^{(b)}$;

10, 11 and 12, 13 stand for the fact that the RRT did not find the violator on the territory with the probability $1 - P_{viol}^{(a)}$ and $1 - P_{viol}^{(b)}$, and the violator did not find the RRT with the probability $1 - P_{gr}^{(a)}$ and $1 - P_{gr}^{(b)}$, respectively;

15 and 18 stand for the fact that stowage devices were detected and eliminated by the RRT with the probability $P_{dev}^{(a)}$ and $P_{dev}^{(b)}$, respectively, but the RRT did not find the violator with the probabilities $1 - P_{viol}^{(a)}$ and $1 - P_{viol}^{(b)}$, and the violator did not find the RRT with the probabilities $1 - P_{gr}^{(a)}$ and $1 - P_{gr}^{(b)}$, while the violator has the ability to intercept speech information using a directional microphone that can be suppressed with the probability $P_{\text{sup}}^{\text{mic}}$;

16 and 17 stand for the fact that the violator is ready to intercept speech information for options “a” and “b” both using a directional microphone and by reading information from stowage devices; probabilities of interference suppression are $P_{\text{sup}}^{\text{mic}}$ and $P_{\text{sup}}^{\text{sd}}$ for a microphone and stowing devices, respectively;

19 and 20 stand for the fact that there are all the necessary conditions for the interception of speech information for options “a” and “b” of the violator’s arrival on the territory;

21 stands for implementation of the threat of interception of speech information during the event;

0 (z), 1 (z) stand for the transitions corresponding to the arrival of the violator to the territory adjacent to the IO before the start of the event and after the start of the event with the probability π_a and π_b, respectively;

2 (z) and 5 (z) stand for the transitions corresponding to the sub-process of detection by the RRT of stowing devices in the corresponding options “a” or “b” of the violator’s arrival on the territory;

3 (z) and 4 (z) stand for the logical “AND” transitions, triggered if the violator did not detect the RRT and the RRT did not find the violator in the corresponding options for violator’s arrival on the territory;

6 (z) and 7 (z) stand for the logical transitions with “AND” logic, triggered if the violator was not detected by the RRT and the RRT did not detect the violator and stowage devices in options “a” or “b” of violator’s arrival on the territory;

8 (z) and 9 (z) stand for the logical transitions with "AND"logic, triggered if stowing devices are detected and eliminated by the RRT, but the violator did not find the RRT and the RRT did not find the violator in the corresponding options for violator’s arrival on the territory;

10 (z) and 11 (z) stand for the logical transitions “OR”, triggered if the violator intercepted information in at least one of the situations of the use of interception means under the conditions of interference for options “a” and “b”;

12 (z) stands for the logical transition of exclusive choice, which is triggered if the threat of information interception is realized either for option “a” or for option “b”.

Let the probabilities that the RRT detects stowing devices and the violator, as well as that the violator detects the RRT in the case when the violator appears on the territory after the start of the event, be proportional to the time remaining until the end of the event. Then:

$$P_{viol}^{(b)} \approx P_{viol}^{(a)} \cdot \overline{\tau_u^{(b)}} \Big/ \overline{\tau_{sp}}, \ \overline{\tau_u^{(b)}} \le \overline{\tau_{sp}}, \ \overline{\tau_u^{(b)}} = \overline{t_{sp}} + \overline{\tau_{sp}} - \overline{t_{tool}}, \overline{t_{sp}} < \overline{t_{tool}} \le \overline{t_{sp}} + \overline{\tau_{sp}}, \tag{14}$$

where $\overline{\tau_u^{(b)}}$, $\overline{\tau_{sp}}$ are the mathematical expectations of the time left for the violator to intercept speech information until the end of the event and duration of the event, respectively. The probabilities $P_{gr}^{(b)}$, $P_{dev}^{(b)}$, $P_{sup}^{(\mathrm{mic},b)}$ are calculated in a similar way.

The time t_u of the realization of the threat of interception of speech information for each of the above i-th situation for both options is the sum of the times $t_{terms}^{(i,a)}$, $t_{terms}^{(i,b)}$ and the time of the threat implementation process since the completion of unsuccessful attempts to expel the violator from the territory and search for stowing devices $\widehat{\tau}_u^{(i,a)}$ and $\widehat{\tau}_u^{(i,b)}$. However, if the values $t_{terms}^{(i,a)}$ and $t_{terms}^{(i,b)}$ can be considered exponentially distributed [19, 20] with the mathematical expectations $\overline{t_{terms}^{(i,a)}}$ and $\overline{t_{terms}^{(i,b)}}$, respectively, then the values $\widehat{\tau}_u^{(i,a)}$ and $\widehat{\tau}_u^{(i,b)}$ are limited by the maximum time of the event conduction $\tau_{sp}^{\max}$ and can be considered uniformly distributed in the interval $\left[0, \tau_{sp}^{max}\right]$ for option a and in the interval $\left[0, \left(\tau_{sp}^{\max} - \tau_u^{(b,\min)}\right)\right]$ for option b, where $\tau_u^{(b,min)} = t_{sp}^{min} + \tau_{sp}^{min} - t_{tool}^{min}$ for $t_{tool}^{min} > t_{sp}^{min}$ and $t_{sp}^{\min}$ and t_{tool}^{min} are the minimum values of the times t_{sp} and t_{tool}.

Expectations $\overline{\widehat{\tau}_u^{(1,a)}}$ and $\overline{\widehat{\tau}_u^{(1,b)}}$ of the random variables $\widehat{\tau}_u^{(i,a)}$ and $\widehat{\tau}_u^{(i,b)}$ are calculated taking into account the setting of acoustic noise as follows:

$$\overline{\widehat{\tau}_u^{(1,a)}} = \frac{\overline{\tau_{\mathrm{sd}}^{(1,a)}} \cdot \overline{\tau_{\mathrm{mic}}^{(1,a)}}}{\left(1 - P_{\mathrm{sup}}^{(\mathrm{mic})}\right) \cdot \overline{\tau_{\mathrm{sd}}^{(1,a)}} + \left(1 - P_{\mathrm{sup}}^{(\mathrm{sd})}\right) \cdot \overline{\tau_{\mathrm{mic}}^{(1,a)}}} \text{ – for the first situation;} \tag{15}$$

$$\overline{\widehat{\tau}_u^{(2,a)}} = \overline{\tau_{\mathrm{mic}}^{(2,a)}} \Big/ \left(1 - P_{\mathrm{sup}}^{(\mathrm{mic})}\right) \text{ – for the second situation,} \tag{16}$$

where $P_{\mathrm{sup}}^{(\mathrm{mic})}$, $P_{\mathrm{sup}}^{(\mathrm{sd})}$ are the probabilities of the suppression of a violator and stowage devices, respectively; $\overline{\tau_{\mathrm{sd}}^{(1,a)}}$, $\overline{\tau_{\mathrm{mic}}^{(1,a)}}$, $\overline{\tau_{\mathrm{mic}}^{(2,a)}}$ are mathematical expectations of time of speech information interception in the absence of acoustic noises with the use of stowage devices and directional microphone for the first situation and only the microphone for the second situation in option "a". The time $\overline{\widehat{\tau}_u^{(1,b)}}$ and $\overline{\widehat{\tau}_u^{(2,b)}}$ is calculated in the similar way. Then the probabilities that the process of interception is continued by the violator in spite of suppression by acoustic noises for option "a", i.e. the probabilities of moving the process from position 16 and 17 to transition 10(z), is determined from the following relations:

$$P_{sup}^{(1,a)} = \frac{\overline{\tau_u^{(1,a)}}}{\overline{\widehat{\tau}_u^{(1,a)}}} = \frac{\left(1 - P_{sup}^{(\mathrm{mic})}\right) \cdot \overline{\tau_{\mathrm{sd}}^{(1,a)}} + \left(1 - P_{sup}^{(\mathrm{sd})}\right) \cdot \overline{\tau_{\mathrm{mic}}^{(1,a)}}}{\overline{\tau_{\mathrm{sd}}^{(1,a)}} + \overline{\tau_{\mathrm{mic}}^{(1,a)}}} \text{ for the first situation;} \tag{17}$$

$$P_{sup}^{(2,a)} = 1 - P_{\mathrm{sup}}^{(\mathrm{mic})} \text{ for the second situation} \tag{18}$$

For option "b" and both situations, the formulas for the calculation are similar.

Mathematical expectations of the times of moving the process from the initial state to the states corresponding to the conditions for the start of interception of speech information are determined using the CPMN, the graph of which is shown in Fig. 3, taking into account two situations corresponding to the composition of the interception means that the violator can use, and in relation to two options for the appearance of a violator on the territory. The indicated states correspond to the positions of the CPMN with numbers 15 – 18. For this, it is necessary to calculate the response time of the logical transitions $6(z), 7(z), 8(z)$ and $9(z)$.

Denote the mathematical expectation of the time of moving the simulated process in the i-th situation by $\overline{t^{(i,a)}_{terms}}$ and $\overline{t^{(i,b)}_{terms}}$ for options a and b, respectively. In this case, $\overline{t^{(1,a)}_{terms}} = \overline{\tau_{0,1}} + \overline{\tau_{6(z)}}$, $\overline{t^{(2,a)}_{terms}} = \overline{\tau_{0,1}} + \overline{\tau_{8(z)}}$, $\overline{t^{(1,b)}_{terms}} = \overline{\tau_{0,0}} + \overline{\tau_{7(z)}}$ and $\overline{t^{(2,b)}_{terms}} = \overline{\tau_{0,0}} + \overline{\tau_{9(z)}}$. Following [7, 19], the response times of transitions 6 (z), 7 (z), 8 (z) and 9 (z) with "AND" logic are calculated at $0 < P^{(a)}_{dev} < 1$ and $0 < P^{(b)}_{dev} < 1$ as follows:

$$\overline{\tau_{6(z)}} = \frac{\left(\frac{\overline{\tau_{2,2}}}{1-P^{(a)}_{dev}} + \overline{\tau_{9,6}}\right)^2 + \left(\frac{\overline{\tau_{2,2}}}{1-P^{(a)}_{dev}} + \overline{\tau_{9,6}}\right) \cdot \left(\overline{\tau_{10,6}} + \overline{\tau_{3(z)}}\right) + \left(\overline{\tau_{10,6}} + \overline{\tau_{3(z)}}\right)^2}{\frac{\overline{\tau_{2,2}}}{1-P^{(a)}_{dev}} + \overline{\tau_{9,6}} + \overline{\tau_{10,6}} + \overline{\tau_{3(z)}}}, \tag{19}$$

$$\overline{\tau_{7(z)}} = \frac{\left(\overline{\tau_{13,7}} + \overline{\tau_{4(z)}}\right)^2 + \left(\overline{\tau_{13,7}} + \overline{\tau_{4(z)}}\right) \cdot \left(\frac{\overline{\tau_{7,5}}}{1-P^{(b)}_{dev}} + \overline{\tau_{14,7}}\right) + \left(\frac{\overline{\tau_{7,5}}}{1-P^{(b)}_{dev}} + \overline{\tau_{14,7}}\right)^2}{\overline{\tau_{13,7}} + \overline{\tau_{4(z)}} + \left(\frac{\overline{\tau_{7,5}}}{1-P^{(b)}_{dev}} + \overline{\tau_{14,7}}\right)}, \tag{20}$$

$$\overline{\tau_{8(z)}} = \frac{\overline{\tau_{1,8}}^2 + \overline{\tau_{1,8}} \cdot \left(\overline{\tau_{11,8}} + \overline{\tau_{3(z)}}\right) \cdot P^{(a)}_{dev} + \left(\overline{\tau_{11,8}} + \overline{\tau_{3(z)}}\right)^2 \cdot P^{(a)2}_{dev}}{\overline{\tau_{1,8}} \cdot P^{(a)}_{dev} + \left(\overline{\tau_{11,8}} + \overline{\tau_{3(z)}}\right) \cdot P^{(a)2}_{dev}}, \tag{21}$$

$$\overline{\tau_{9(z)}} = \frac{\overline{\tau_{8,9}}^2 + \overline{\tau_{8,9}} \cdot \left(\overline{\tau_{12,9}} + \overline{\tau_{4(z)}}\right) \cdot P^{(b)}_{dev} + \left(\overline{\tau_{12,9}} + \overline{\tau_{4(z)}}\right)^2 \cdot P^{(b)2}_{dev}}{\overline{\tau_{8,9}} \cdot P^{(b)}_{dev} + \left(\overline{\tau_{12,9}} + \overline{\tau_{4(z)}}\right) \cdot P^{(b)2}_{dev}}. \tag{22}$$

Taking into account the fact that movement from the transition to the position occurs instantly, the movement of the simulated process in positions 10 and 11 is determined by the response time of the logical transition 3(z) with the logic "AND", which means the times of the movement of the process from positions 3 and 4 to the transition 3(z), that is, the times during which the RRT does not detect the violator, and the violator does not detect the RRT, which are calculated as follows [19]:

$$\overline{\tau_{3,3}} = \overline{\tau^{(0)}_{3,3}} \Big/ \left(1 - P^{(a)}_{viol}\right),\ P^{(a)}_{viol} < 1;\ \ \overline{\tau_{4,3}} = \overline{\tau^{(0)}_{4,3}} \Big/ \left(1 - P^{(a)}_{gr}\right),\ P^{(a)}_{gr} < 1, \tag{23}$$

where $\overline{\tau^{(0)}_{3,3}}$ and $\overline{\tau^{(0)}_{4,3}}$ are mathematical expectations of time of moving the process from positions 3 and 4 to transition 3(z) in the cases when the RRT detects the violator and the violator detects the RRT with the probabilities equal to 1. Then the mathematical expectations of the response times of the logical transitions $3(z)$, $4(z)$ with the logic "AND" are calculated by the formulas [7, 19]:

$$\overline{\tau_{3(z)}} = \frac{\overline{\tau_{3,3}}^2 + \overline{\tau_{3,3}} \cdot \overline{\tau_{4,3}} + \overline{\tau_{4,3}}^2}{\overline{\tau_{3,3}} + \overline{\tau_{4,3}}}, \tag{24}$$

$$\overline{\tau_{4(z)}} = \frac{\overline{\tau_{5,4}}^2 + \overline{\tau_{5,4}} \cdot \overline{\tau_{6,4}} + \overline{\tau_{6,4}}^2}{\overline{\tau_{5,4}} + \overline{\tau_{6,4}}},\ \overline{\tau_{6,4}} = \frac{\overline{\tau^{(0)}_{6,4}}}{1 - P^{(b)}_{viol}},\ P^{(b)}_{viol} < 1;\ \ \overline{\tau_{5,4}} = \frac{\overline{\tau^{(0)}_{5,4}}}{1 - P^{(b)}_{gr}},\ P^{(b)}_{gr} < 1. \tag{25}$$

In addition, the mathematical expectations of the times of moving the process from position 2 to transition 2(z) and from position 7 to transition 5(z) are determined from the relations

$$\overline{\tau_{2,2}} = \overline{\tau^{(0)}_{2,2}} \Big/ (1 - P_{dev}),\ P_{dev} < 1;\ \ \overline{\tau_{7,5}} = \overline{\tau^{(0)}_{7,5}} \Big/ (1 - P_{dev}),\ P_{dev} < 1, \tag{26}$$

and the times of movement from position 1 to transition 8(z) and from position 8 to transition 9(z) are determined from the relations

$$\overline{\tau_{1,8}} = \overline{\tau^{(0)}_{1,8}} \Big/ P_{dev},\ P_{dev} < 1;\ \ \overline{\tau_{8,9}} = \overline{\tau^{(0)}_{8,9}} \Big/ P_{dev},\ P_{dev} < 1. \tag{27}$$

Uniform distribution of $\widehat{\tau}_u^{(i,a)}$ and $\widehat{\tau}_u^{(i,b)}$ stipulates that the subprocesses after positions 15 – 17 are neither Markov nor semi-Markov. In this case, the probability that the threat of interception is realized in time t for the i-th situation ($i = \overline{1,2}$) and the option a of the violator's appearance, that is, the inequality $t_u \leq t$ holds, is found as follows [14]:

$$P_u^{(i,a)}(t) = \begin{cases} 0 \quad \text{for t} \leq 0; \\ \left[1 - P_{\text{sup}}^{(i,a)}\right] \cdot \left[\dfrac{t}{\tau_{sp}^{\max}} - \dfrac{1-e^{-\frac{t}{\overline{t_{terms}^{(i,a)}}}}}{\tau_{sp}^{\max}} \cdot \overline{t_{terms}^{(i,a)}}\right] & \text{for} \quad 0 < t \leq \tau_{sp}^{(\max)}; \\ \left[1 - P_{\text{sup}}^{(i,a)}\right] \cdot \left[1 - \dfrac{1-e^{-\frac{\tau_{sp}^{(\max)}}{\overline{t_{terms}^{(i,a)}}}}}{\tau_{sp}^{\max}} \cdot \overline{t_{terms}^{(i,a)}}\right] & \text{for} \quad \tau_{sp}^{(\max)} < t, \end{cases} \tag{28}$$

where $P_{\text{sup}}^{(i,a)}$ stands for the probabilities calculated for the first ($i = 1$) and for the second ($i = 2$) situations by formulas (17) and (18). Similarly, the probability $P_u^{(i,b)}(t)$ is calculated for option b, where the value $\overline{t_{terms}^{(i,b)}}$ is used instead of $\overline{t_{terms}^{(i,a)}}$, and the value $\tau_{sp}^{\max} - \tau_u^{(b,\min)}$ is used instead of $\tau_{sp}^{\max}$.

The probability that information is intercepted in at least one of the situations for options "a" and "b" is calculated by the formula:

$$P_u^{(a)}(t) = 1 - \prod_{i=1}^{2}\left[1 - P_u^{(i,a)}(t)\right] \quad \text{and} \quad P_u^{(b)}(t) = 1 - \prod_{i=1}^{2}\left[1 - P_u^{(i,b)}(t)\right]. \tag{29}$$

Then the probability of interception of speech information during the event at the IO is determined as follows:

$$P_u(t) = \pi_a \cdot P_u^{(a)}(t) + \pi_b \cdot P_u^{(b)}(t) \tag{30}$$

Example 1. It is necessary to calculate the probability of realizing the threat of speech information leakage through the acoustic channel during a meeting on business matters with the following initial data.

The minimum and maximum meeting time is $\tau_{sp}^{(\min)} = 1$ hour and $\tau_{sp}^{(\max)} = 2$ hours, that is, the average time is $\overline{\tau_{sp}} = 1,5$ hours. The waiting time for the beginning of the meeting is from 20 to 80 minutes, that is, on average $\overline{t_{sp}} = 50$ min. The minimum $t_{tool}^{\min}$ and the maximum $t_{tool}^{\max}$ time of the violator's arrival on the territory adjacent to the IO are 30 and 90 minutes, respectively, that is, the average time is $\overline{t_{tool}} = 60$ min. In this case, $\pi_a = \frac{50}{50+60} = 0,45$, $\pi_b = \frac{60}{60+50} = 0,55$ and $\overline{\tau_u^{(b)}} = 80$ min. The RRT starts searching for the violator and stowage devices from the beginning of the working day. Let the probability of detecting a violator be $P_{viol}^{(a)} = 0,8$, the probability that the violator detects the RRT be $P_{gr}^{(a)} = 0,9$, and suppose that detection of stowage devices is possible with the probability $P_{dev}^{(a)} = 0,9$. The use of an acoustic noise generator leads to the suppression of a directional microphone and stowing devices with the probabilities $P_{\text{sup}}^{(\text{mic})} = 0,6$ and $P_{\text{sup}}^{(\text{sd})} = 0,9$ respectively. Then, in accordance with relation (14), $P_{viol}^{(b)} = 0,71$, $P_{gr}^{(b)} = 0,8$, $P_{dev}^{(b)} = 0,8$.

The times for moving the process from positions to transitions have the following values: $\overline{\tau_{0,0}} = \overline{\tau_{0,1}} \approx 0$ min, $\overline{\tau_{1,8}} = \overline{\tau_{2,2}} = \overline{\tau_{7,5}} = \overline{\tau_{8,9}} = 20$ min, $\overline{\tau_{4,3}^{(0)}} = \overline{\tau_{5,4}^{(0)}} = 10$ min $\overline{\tau_{15,11}} = \overline{\tau_{18,11}} = \overline{\tau_{16,10}} = \overline{\tau_{17,10}} \approx 0$ min, $\overline{\tau_{3,3}^{(0)}} = \overline{\tau_{6,4}^{(0)}} = 15$ min, $\overline{\tau_{9,6}} = \overline{\tau_{10,6}} = \overline{\tau_{11,8}} \approx 0$ min, $\overline{\tau_{13,7}} = \overline{\tau_{14,7}} = \overline{\tau_{12,9}} \approx 0$.

Based on the calculation results, we obtain: $\overline{\tau_{\text{sd}}^{(1,a)}} = \overline{\tau_{\text{mic}}^{(1,a)}} = \overline{\tau_{\text{mic}}^{(2,a)}} = 60$ min, $\overline{\tau_{\text{sd}}^{(1,b)}} = \overline{\tau_{\text{mic}}^{(1,b)}} = \overline{\tau_{\text{mic}}^{(2,b)}} = 80$ min, $\widehat{\tau}_u^{(1,a)} = 120$ min, $\widehat{\tau}_u^{(2,a)} = 150$ min, $\widehat{\tau}_u^{(1,b)} = 160$ min, $\widehat{\tau}_u^{(2,b)} =$

200 min, $\overline{t_{terms}^{(1,a)}} = 252$ min, $t_{terms}^{(2,a)} = 134$ min, $\overline{t_{terms}^{(1,b)}} = 133$ min $\overline{t_{terms}^{(2,b)}} = 84$ min and $\tau_u^{(b,\min)} = 50$ min. Based on the obtained values of the response times of the CPMN transitions of formulas (28) and (29), in accordance with (30), the time dependence of the probability to realize the threat of speech information leakage for both options of the violator's appearance on the territory during the event in the IO was calculated, see Fig. 4.

Therefore, the proposed approach to taking into account the temporal characteristics of events, actions to protect information, actions of a violator to intercept information allows to increase significantly the accuracy of assessing the possibilities of information leakage through TCIL in comparison with the approach used today, which is based on calculating only the energy characteristics of transmitted and intercepted signals.

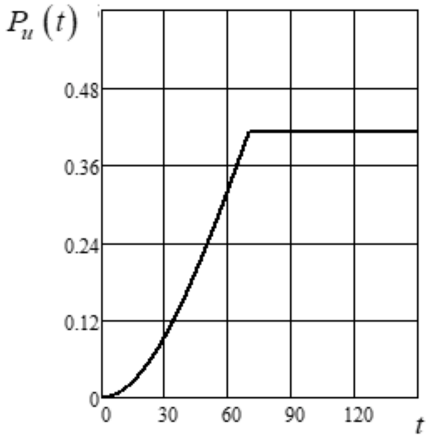

Fig. 4. Time dependence of the probability to realize the threat of speech information leakage, taking into account both options of the violator's appearance on the territory

Conclusion

1. Analysis of expressions (28) – (30) and the above graph showed that the probability of interception depends significantly on the time parameters of both the conduct of the event and the actions of the RRT, and the actions of the violator. Failure to take into account the time factor when assessing the possibility of information leakage through the TCIL leads to significantly overestimated estimates of the possibility of its interception.

2. The time of interception of information is limited not only by the time of the event, the operation of devices, the application of protective measures, etc., but also by the probabilistic and temporal characteristics of the violator's actions. At the same time, the reduction in the time spent by the violator in the territory adjacent to the IO leads to a reduction in the volume of intercepted information, but can increase the possibility of interception, since this significantly reduces the probabilities of detecting a violator and functioning stowing devices for intercepting information through TCIL.

3. Under the sufficient energy conditions, the use of interference (acoustic, vibroacoustic, electromagnetic, etc.) can lead to the exclusion of the possibility of intercepting the protected information through the TCIL. In this case, it is not necessary to take into account the time factor when assessing the possibility of information leakage through the TCIL. However, such measures are not always advisable, and in practice such measures are used only when other organizational and organizational-technical measures are insufficient, which, as a rule, is revealed by expert analysis. Further development of the proposed approach will make it possible to move from expert to quantitative assessments of the possibility of intercepting information through the TCIL, taking into account the time factor.

References

1. Bandyopadhyay S., Sarkar D., Mandal C. Equivalence Checking of Petri Net Models of Programs Using Static and Dynamic Cut-Points. *Acta Informatica*, 2019, vol. 56, no. 4, pp. 321–383.
2. Ahmedov M.A., Rahimov S.R., Mustafayev V.A., Atayev G.N. Simulation of Dynamical Enterprises Process with Application of the Modification Fuzzy Net Petri. *Advances in Intelligent Systems and Computing*, 2017, no. 502, pp. 913–920.
3. Stetsenko I.V., Dyfuchyna O. Simulation of Multithreaded Algorithms Using Petri-Object Models. *Advances in Intelligent Systems and Computing*, 2019, no. 754, pp. 391–401.
4. Karyotis V., Khouzani M.H.R. *Malware Diffusion Models for Wireless Complex Networks. Theory and Applications.* Amsterdam, Elsevier, 2015.
5. Georgiadis S., Limnios N. Nonparametric Estimation of the Stationary Distribution of a Discrete-Time Semi-Markov Process. *Communications in Statistics – Theory and Methods*, 2015, vol. 44, no. 7, pp. 1319–1337.
6. Brissaud F., Luiz F. Average Probability of a Dangerous Failure on Demand: Different Modelling Methods, Similar Results. *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference*, 2012, pp. 6073–6082.
7. Yazov Yu.K., Tekunov V.V. Modeling the Dynamics of the Implementation of Threats to Information Security Using the Apparatus of Petri–Markov Nets. *Information and Safety: Scientific Journal*, 2018, vol. 17, no. 3, pp. 464–467. (in Russian)
8. Avsentev O.S., Avsentev A.O., Yazov Yu.K., Rubtsova I.O. Method for Evaluating the Effectiveness of Protection of Electronic Document Management Using the Apparatus of Petri–Markov Nets. *Proceedings of SPIIRAS*, 2019, vol. 18, no. 6, pp. 1269–1300. (in Russian)
9. Yamamoto K., Nakagawa S. Privacy Protection for Speech Information. *Journal of Information Assurance and Security*, 2010, no. 5, pp. 284–292.
10. Avsentev A.O., Krugov A.G., Perova Yu.P. Functional Models of Information Protection Against Leakage Due to Side Electromagnetic Radiation of Informatization Objects. *Proceedings of TUSUR*, 2020, vol. 22, no. 2, pp. 29–39. (in Russian)
11. Avdeev V.B., Katrusha A.N. Calculation of the Attenuation Coefficient of Spurious Electromagnetic Radiation. *Special Equipment*, 2013, no. 2, pp. 18–27. (in Russian)
12. Antipov D.A., Shelupanov A.A. Investigation of the Directivity of Side Electromagnetic Radiation from a Personal Computer. *Proceedings of TUSUR*, 2018, no. 2, pp. 33–37. (in Russian)
13. Horev A.A. PAK for Detecting Electronic Devices for Intercepting Speech Information. *Protection of Information. Inside*, 2018, no. 1, pp. 207–213. (in Russian)
14. Avsentiev O.S., Avsentiev A.O., Krugov A.G., Yazov Yu.K. Simulation of Processes of Information Protection of Informatization Objects from Leakage on Technical Channels Using a Petri–Markov Network Apparatus. *Journal of Computational and Engineering Mathematics*, 2021, vol. 8, no. 2, pp. 32–41.
15. Avdeev V.B., Anischenko A.V. Application of Frequency-Selective Detectors of Laser Radiation to Protect Speech Information from Its Leakage Through a Laser Channel. *Telecommunications*, 2020, no. 2, pp. 24–30. (in Russian)
16. Avdeev V.B., Anishchenko A.V., Petigin A.F., Dergachev Yu.A. Estimation of the Radio Transmission Range of Signals from a Computer Using Its Spurious Electromagnetic Radiation. *Telecommunications*, 2020, no. 9, pp. 2–10. (in Russian)

17. Avdeev V.B., Akimov E.L., Anishchenko A.V., Berdyshev A.V., Pyrochkin S.A. Investigation of the Coefficients of Acousto-Vibration Transformation of Speech Signals on Objects in the Laser Channel for Intercepting Information. *Telecommunications*, 2020, no. 8, pp. 8–13. (in Russian)

18. Horev A.A., Korolenko M.K., Serov F.S., Porsev I.S. Research of Detection Probability (Audibility) of Signals in Octave Bands. *Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering*, 2020, pp. 2057–2061.

19. Yazov Yu.K., Anischenko A.V. *Seti Petri – Markova i ikh primeneniye dlya modelirovaniya protsessov realizatsii ugroz bezopasnosti informatsii v informatsionnykh sistemakh* [Petri–Markov Nets and Their Application for Modelling the Processes of Implementation of Threats to Information Security in Information Systems]. Voronezh, Kvarta, 2020. (in Russian)

20. Ignatiev V.M., Larkin E.V. *Seti Petri–Markova* [Petri–Markov Nets]. Tula, TulGTU, 1997. (in Russian)

Received January 25, 2021

УДК 621.3 **DOI: 10.14529/mmp210404**

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ С ПРИМЕНЕНИЕМ АППАРАТА СЕТЕЙ ПЕТРИ – МАРКОВА

***О.С. Авсентьев*[1]*, А.О. Авсентьев*[1]*, А.Г. Кругов*[2]*, Ю.К. Язов*[3]**

[1]Воронежский институт МВД России, г. Воронеж, Российская Федерация

[2]Управление вневедомственной охраны войск национальной гвардии по Тверской области, г. Тверь, Российская Федерация

[3]Воронежский государственный технический университет, г. Воронеж, Российская Федерация

Предлагается подход к моделированию процессов защиты информации на объектах информатизации в динамике реализации угроз ее утечки по техническим каналам с применением аппарата составных сетей Петри – Маркова. Исследуются взаимосвязи процессов передачи информации на объекте информатизации, ее перехвата нарушителем из-за пределов этого объекта по техническим каналам и защиты от перехвата. Получены аналитические выражения для расчета вероятностно-временных характеристик моделируемых процессов в интересах оценки возможности реализации нарушителем угроз утечки информации на объектах информатизации; защиту этой информации за счет применения превентивных мер, направленных на блокирование или опережение действий нарушителя по реализации этих угроз.

Ключевые слова: технический канал утечки информации; защита информации; превентивная мера защиты; эффективность защиты; вероятностно-временная характеристика; разветвляющийся процесс; логическое условие; моделирование процесса; составная сеть Петри – Маркова.

Литература

1. Bandyopadhyay, S. Equivalence Checking of Petri Net Models of Programs Using Static and Dynamic Cut-Points / S. Bandyopadhyay, D. Sarkar, C. Mandal // Acta Informatica. – 2019. – V. 56, № 4. – P. 321–383.
2. Ahmedov, M.A. Simulation of Dynamical Enterprises Process with Application of the Modification Fuzzy Net Petri / M.A. Ahmedov, S.R. Rahimov, V.A. Mustafayev, G.N. Atayev // Advances in Intelligent Systems and Computing. – 2017. – № 502. – P. 913–920.
3. Stetsenko, I.V. Simulation of Multithreaded Algorithms Using Petri-Object Models / I.V.Stetsenko, O. Dyfuchyna // Advances in Intelligent Systems and Computing. – 2019. – № 754. – P. 391–401.
4. Karyotis, V. Malware Diffusion Models for Wireless Complex Networks. Theory and Applications / V. Karyotis, M.H.R. Khouzani. – Amsterdam: Elsevier, 2015.
5. Georgiadis, S. Nonparametric Estimation of the Stationary Distribution of a Discrete-Time Semi-Markov Process / S. Georgiadis, N. Limnios // Communications in Statistics – Theory and Methods. – 2015. – V. 44, № 7. – P. 1319–1337.
6. Brissaud, F. Average Probability of a Dangerous Failure on Demand: Different Modelling Methods, Similar Results / F. Brissaud, F. Luiz // 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference. – 2012. – P. 6073–6082.
7. Язов, Ю.К. Моделирование динамики реализации угроз безопасности информации с использованием аппарата сетей Петри – Маркова / Ю.К. Язов, В.В. Текунов // Информация и безопасность. – 2018. – Т. 17, № 3. – С. 464–467.
8. Авсентьев, О.С. Метод оценивания эффективности защиты электронного документооборота с применением аппарата сетей Петри – Маркова / О.С. Авсентьев, А.О. Авсентьев, Ю.К. Язов, И.О. Рубцова // Труды СПИИРАН. – 2019. – Т. 18, № 6. – С. 1269–1300.
9. Yamamoto, K. Privacy Protection for Speech Information / K. Yamamoto, S. Nakagawa // Journal of Information Assurance and Security. – 2010. – № 5. – P. 284–292.
10. Авсентьев, А.О. Функциональные модели защиты информации от утечки за счет побочных электромагнитных излучений объектов информатизации / А.О. Авсентьев, А.Г. Кругов, Ю.П. Перова // Доклады ТУСУР. – 2020. – Т. 22, № 2. – С. 29–39.
11. Авдеев, В.Б. Расчет коэффициента ослабления побочных электромагнитных излучений / В.Б. Авдеев, А.Н. Катруша // Специальная техника. – 2013. – № 2. – С. 18–27.
12. Антипов, Д.А. Исследование направленности побочного электромагнитного излучения от персонального компьютера / Д.А. Антипов, А.А. Шелупанов // Доклады ТУСУР. – 2018. – № 2. – С. 33–37.
13. Хорев, А.А. ПАК для выявления электронных устройств перехвата речевой информации / А.А. Хорев // Защита информации. Инсайд. – 2018. – № 1. – С. 207–213.
14. Avsentiev, O.S. Simulation of Processes of Information Protection of Informatization Objects from Leakage on Technical Channels Using a Petri–Markov Network Apparatus / O.S. Avsentiev, A.O. Avsentiev, A.G. Krugov, Yu.K. Yazov // Journal of Computational and Engineering Mathematics. – 2021. – V. 8, № 2. – P. 3–24.
15. Авдеев, В.Б. Применение частотно-селективных обнаружителей лазерного излучения для защиты речевой информации от ее утечки по лазерному каналу / В.Б. Авдеев, А.В. Анищенко // Телекоммуникации. – 2020. – № 2. – С. 24–30.

16. Авдеев, В.Б. Оценка дальности радиопередачи сигналов с компьютера с использованием его побочного электромагнитного излучения / В.Б. Авдеев, А.В. Анищенко, А.Ф. Петигин, Ю.А. Дергачев // Телекоммуникации. – 2020. – № 9. – С. 2–10.

17. Авдеев, В.Б. Исследование коэффициентов акустовибрационного преобразования речевых сигналов на объектах в лазерном канале перехвата информации / В.Б. Авдеев, Е.Л. Акимов, А.В. Анищенко, А.В. Бердышев, С.А. Пырочкин // Телекоммуникации. – 2020. – № 8. – С. 8–13.

18. Horev, A.A. Research of Detection Probability (Audibility) of Signals in Octave Bands / A.A. Horev, M.K. Korolenko, F.S. Serov, I.S. Porsev // Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering. – 2020. – P. 2057–2061.

19. Язов, Ю.К. Сети Петри – Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах / Ю.К. Язов, А.В. Анищенко. – Воронеж: Кварта, 2020.

20. Игнатьев, В.М. Сети Петри – Маркова / В.М. Игнатьев, Е.В. Ларкин. – Тула: ТулГТУ, 1997.

Олег Сергеевич Авсентьев, доктор технических наук, профессор, кафедра информационной безопасности, Воронежский институт МВД России (г. Воронеж, Российская Федерация), osaos@mail.ru.

Александр Олегович Авсентьев, кандидат технических наук, старший преподаватель, кафедра физики и радиоэлектроники, Воронежский институт МВД России (г. Воронеж, Российская Федерация), aoaao8787@mail.ru.

Артем Геннадьевич Кругов, заместитель начальника отдела организации внедрения и эксплуатации технических средств охраны и безопасности, управление вневедомственной охраны войск национальной гвардии по Тверской области (г. Тверь, Российская Федерация), krtemik@gmail.com.

Юрий Константинович Язов, доктор технических наук, профессор, кафедра систем информационной безопасности, Воронежский государственный технический университет (г. Воронеж, Российская Федерация), yazoff_1946@mail.ru.

Поступила в редакцию 25 января 2021 г.