ENGINEERING MATHEMATICS

MSC 68T05, 62J07, 68Q32 **DOI: 110.14529/jcem210201**

SIMULATION OF PROCESSES FOR PROTECTING VOICE INFORMATION OBJECTS AGAINST LEAKAGE THROUGH THE SPURIOUS ELECTROMAGNETIC RADIATION CHANNELS USING THE PETRI – MARKOV NETS

O. S. Avsentev[1], osaos@mail.ru,
A. O. Avsentev[1], aoaao8787@mail.ru,
A. G. Krugov[2], krtemik@gmail.com,
Yu. K. Yazov[3], yazoff_1946@mail.ru
[1]Voronezh Institute of the Ministry of the Interior of the Russian Federation, Voronezh, Russian Federation,
[2]Department of Private Security of the National Guard Troops in the Tver Region, Tver, Russian Federation,
[3]Voronezh State Technical University, Voronezh, Russian Federation

In order to assess quantitatively the protection of information on objects of informatization (OI) against leakage through channels of spurious electromagnetic radiation (SEMR), we propose to simulate the processes of interception of SEMR using the apparatus of Petri – Markov nets, which makes it possible to take into account the probabilistic-temporal characteristics of parallel processes of interception of such radiations arising in radio electronic devices (RED) of structural elements (SE) of an object, actions of a violator implementing interception from outside of the controlled area (CA), as well as protective measures aimed at preventing the possibility of intercepting SEMR. It is assumed that the energy and frequency characteristics of the SEMR allow a violator to carry out such an interception in the absence of protective measures. Indicators of assessment are given and analytical dependencies for their calculation are obtained. The model allows to assess the possibility of intercepting information related to confidential in time, as well as the impact of protective measures on the violator ability to intercept SEMR containing information of a confidential nature. We give examples of calculating the proposed indicators when analyzing the protection of voice information against interception by SEMR of RED of OI, and estimate the influence of preventive organizational and technical protection measures on reducing the possibilities of interception depending on the efficiency and timing of their implementation. Based on the performed computational experiment, we show that, when analyzing the protection of voice information against leakage by SEMR, it is necessary to evaluate not only the possibilities of energy detection of SEMR, but also the possibility of intercepting SEMR in time.

Keywords: information security indicator; spurious electromagnetic radiation; Petri – Markov net; preventive measures for information protection; technical channel of information leakage; time characteristics.

Abbreviations

CA – controlled area
IPr – information processes
ISS – information security system
OI – objects of informatization
PII – process of intercepting information
PIP – process of information protection
PMN – Petri – Markov net
RED – radio electronic devices
RRT – rapid response teams
SE – structural elements
SEMR – spurious electromagnetic radiation
TCIL – technical channel of information leakage
TM – technical means

Introduction

At present, the requirements and measures for the protection of confidential information on OI against leakage by SEMR of RED by international standards [1] adopted in the Russian Federation in an authentic translation [2] are not regulated. At the same time, a wide variety of OIs is associated with differences in the types of information, a wide range of SEs in their composition, the presence of various kinds of REDs that can act as sources of SEMR, and allows a violator to use these emissions to intercept information containing confidential information. The choice of adequate protection measures against such interception depends on both the energy factors (the power of the SEMR, the sensitivity of the violator receiver, the distance between the RED and the violator, the characteristics of the propagation medium, etc.) and the duration of messages converted in the SEMR in the RED, as well as the time available for a violator to deploy and configure a receiving equipment and intercept SEMR. However, nowadays the methodological support of the specified choice of protection measures is focused on taking into account energy characteristics only.

So, in [3, 4], instrumental and computational methods are used as a methodological support for the choice of protection measures. The works [5, 6] investigate the physical processes of propagation of radio waves of various ranges in the atmosphere and near the earth's surface. In turn, the work [7] considers the essence and features of the application of information protection measures under the conditions of intercepting the radiation of informative signals using hardware and software radio control systems. The conclusion about the need to apply measures to protect information against leakage is made on the basis of calculations of the energy characteristics of the informative signal during its propagation in the air from the RED of OI to the technical means (TM) of interception used by the violator outside the CA. At the same time, this does not take into account the time characteristics of both the actions of the violator to intercept the SEMR, and the time of existence of information in the OI, as well as the set of functions implemented during the application of the necessary protection measures.

Failure to take into account the time factor leads, as a rule, to overestimated information protection as the ability of its protection system to withstand the threat

of leakage. This is due to the fact that the failure to meet the energy conditions under which there is no possibility of intercepting the spurious signals of the RED does not mean that the violator is able to intercept the necessary information. In addition, sometimes, it is very difficult to fulfill the specified conditions, since the possibility of intercepting information by SEMR depends on many factors: the presence of REDs in the OI, which can act as sensors of the intercepted information; the existence of links between SEMR and confidential information circulating in the OI; the extent of the medium of propagation of these signals outside the CA of the object, at which it is possible to use a receiver to intercept them taking into account its sensitivity; the presence of conditions on the territory adjacent to the CA for the secret execution of actions by the violator to use this receiver. In turn, under these conditions, counteraction to the interception of information is possible through the use of preventive measures to protect it of an organizational and technical nature [8] aimed at blocking the indicated actions of the violator.

The dynamics of each of these processes can be characterized by their temporal characteristics: the time of beginning, completion and duration of implementation. These times are random variables that makes it difficult to solve the problem on taking into account these characteristics when assessing the protection of information in the OI against leakage by the technical channel of information leakage (TCIL) of the considered type in the interests of choosing adequate protection measures.

These circumstances necessitate the use of methods for quantitatively assessing the protection of information of the OI against leakage by SEMR with the development of an appropriate mathematical model.

In theoretical terms, the study of the issues of assessing the protection of information of OI against leakage due to SEMR of their RED, taking into account the dynamics of the implementation of processes of the type under consideration and their interrelationships, are of a limited nature. Most scientific publications propose various approaches to its assessment, which are aimed at studying individual elements of the description of TCIL and the formation of an information security system (ISS) on this basis.

For example, the work [9] proposes an expert approach to assessing the protection of information against threats of leakage through SEMR channels and pickups. The approach is based on the implementation of empirical procedures for systematizing the relationships between sources of information leakage threats and its vulnerabilities. In this case, the security of information is assessed according to the probabilistic indicator of assessing the level of threat.

Also, qualitative approaches were developed, in which the process of protecting information against interception due to SEMR is characterized by a certain quality considered as a result of the performance of the target protection function, which allows its functional representation [10]. Each of the many functions that make up the multilevel structure of the functional description of the processes under study is implemented by performing a certain sequence of actions characterized by the times of their execution. However, since actions can be performed both sequentially and in parallel, there are difficulties in determining the numerical value of the total time of implementation of the objective function and the information security indicator that takes this time into account.

The apparatus of Petri nets [11–14] was found wide application for modelling branching processes. Currently, Petri nets (PRES+ models [11], fuzzy Petri nets of the type *Vf* [12], stochastic Petri nets [13], networks simulating the spread of malicious programs in various

wireless complex networks [14]) are used to develop simulation models of various kinds of branching processes mainly. Their use for these purposes is associated with significant labor costs and leads to great difficulties in accounting for the time factor.

Recently, in the interests of taking into account the time factor when assessing the security of information of the OI against leakage due to SEMR, more and more attention is paid to the use of the apparatus of Markov or semi-Markov processes [15]. However, at the same time, significant difficulties arise due to the need to take into account the dynamics of parallel implemented partial processes that make up the process of realizing the threat of interception of SEMR, as well as the logical conditions for such an implementation. For example, the process of intercepting information (PII) with the help of a TM can be implemented under the conditions when the information to be protected and the corresponding SEMR in the RED appear, the SEMR have energy characteristics that allow identifying information with a sufficient level of its quality, this information contains the information the violator needs, the violator installed and configured TM for intercepting SEMR, etc. At the same time, the process of information protection (PIP) against leakage by SEMR can be implemented by using the ISS formed in advance both independently of the implementation of the PII and with the use of additional preventive measures for protecting information taking into account the actions of the violator implementing the PII.

It is practically impossible to take into account these factors analytically using the traditional apparatus of Markov and semi-Markov processes [16, 17]. In a similar situation, in order to provide the possibility of analytical calculation of information security indicators of OI in relation to information systems of electronic document management, the work [18] proposes to use the apparatus of Petri – Markov nets.

In this work, we propose to use the apparatus of Petri – Markov nets to assess the security of voice information against leakage due to the SEMR of the RED of the OI.

In [19], it is shown that for the use of this apparatus in the interests of assessing the security of information against leakage, it is advisable to preliminarily develop descriptive models that include a set of actions performed during the implementation of information processes (IPr) in OI and PII under the conditions of applying preventive information protection measures aimed to block the violator actions to implement its interception according to the SEMR of the RED of the OI. At the same time, the timely response of the ISS to the actions of the violator to implement the PII is considered as the goal of protection, and probabilistic or average statistical indicators are used as indicators.

1. Descriptive Model of the Process of Forming Conditions for Intercepting Voice Information by SEMR

When developing descriptive models of implementation of threats of intercepting SEMRs containing voice information of a confidential nature, the following is taken into account.

1. Events, during which leakage of such information by SEMR is possible, are carried out during the working day at a time unknown for the violator. The interception of the SEMR by the violator is a random process in time.

2. Before the start of the event, the equipment for sound amplification, sound recording, sound reproduction, video recording and playback, terminal devices that function until the

end of the event are turned on and adjusted.

3. Only fragments of the speeches of the participants of the event contain information of a confidential nature. Moreover, the time of occurrence of such fragments and their duration are random.

4. The time during which a violator can intercept a SEMR is limited and random, since a violator cannot be near the controlled territory for a long time due to the danger of detecting himself.

5. Before intercepting voice information, the violator carries out a number of actions such as scanning the frequency range in order to detect the SEMR of the RED, determining the direction of the maximum level of their radiation [5], choosing a place for the covert use of a TC at a minimum distance to the boundaries of the CA of the OI, determining the type of the SEMR signal, and the width of its spectrum, setting the mode of operation of the TM corresponding to the type of intercepted information. The execution times of these actions are random values. In this case, leakage can occur through the SEMR of one of several REDs of the OI, for the radiation of which the violator's TM receiver is adjusted.

6. Organizational and technical measures can be applied to protect voice information against leakage by SEMR. Organizational measures include the use of mobile rapid response teams (RRT), that are patrol groups of 2 – 3 people to patrol the territory adjacent to the OI of the CA. The management of these groups is carried out by the ISS administrator, who controls the operational situation in this area using video surveillance systems. The RRT conduct an inspection of the adjacent territory to find the place from which the violator intercepts the SEMR. The technical measures include the use of mobile devices that simulate false SEMRs and mobile noise generators, which are used to equip the patrol RRT.

7. The effect of protection is achieved due to the following facts. First, a patrol group appears within sight of the violator, which causes the termination of the violator actions to intercept the SEMR and removing the violator from the territory adjacent to the CA. Second, RRT use mobile technical means of active protection in order to exclude the possibility of information leakage. Both organizational and technical measures are anticipatory and turn out to be effective if, as a result of their use, the violator does not have time to intercept the SEMR by which he can reveal confidential voice information. These measures are applied in practice, but other measures are also possible, for example, those indicated in [19].

2. Indicators for Assessing the Security of Voice Information against Leakage Through the Channels of Spurious Electromagnetic Radiation

Since almost all the processes taken into account in the implementation of the threat of voice information leakage due to the SEMR of the RED of the OI are random in time, it is advisable to use the probability of the threat realization in a given time as an indicator for assessing the security by analogy with [18]. Such a leak can occur only during the time of delivering a speech, or during a certain fraction of this time, which is sufficient for the disclosure of confidential information. The possibility of a leak is caused not only by the length of the speech of the event participant, but also by the readiness of the violator to

intercept the SEMR. In this case, it is assumed that the version of the violator's actions, which is worst for the legitimate user of the OI takes place, when, within the time t_{tool}, the violator moves to the territory adjacent to the CA, deploys and sets up the interception TM until the moment t_{act}, corresponding to the beginning preparation for the event, that is, before switching on and setting up the sound reinforcement system (Fig. 1).

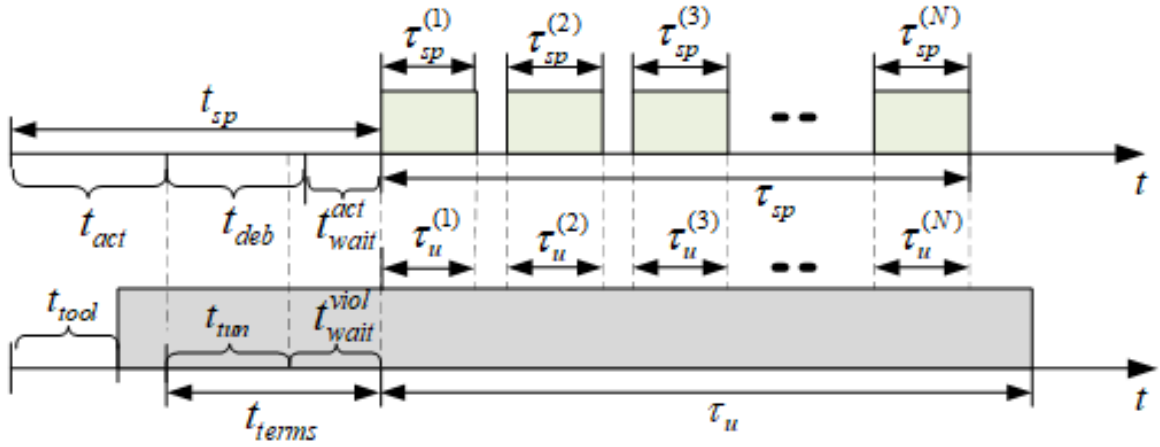

Fig. 1. The ratio of the times of preparation and holding an event and the actions of the violator

In Fig. 1, the following symbols are used:

t_{tool} is a time from the beginning of the working day to the moment the violator deployed the interception TM;

t_{tun} is a time of the TM tuning for SEMR interception;

t_{sp} is a time of waiting for the start of the event, that is, the time before the start of the first participant of the event (the time consists of the time from the beginning of the working day to the start of preparation for the event denoted by t_{act}, the duration of setting up the sound reinforcement system denoted by t_{deb} and the time of waiting for the first participant of the event denoted by t_{wait}^{act});

τ_{sp} is a duration of the event;

$\tau_{sp}^{(1)}$, $\tau_{sp}^{(2)}$, $\tau_{sp}^{(3)}$... $tau_{sp}^{(N)}$ are durations of the performances of the event participants;

t_{terms} is a time required for the formation of interception conditions by the violator (t_{tun} that is deployment the interception TM and its setting in the territory adjacent to the CA, as well as the violator's waiting for the start of the event denoted by t_{wait}^{viol}) during the time of deployment and tuning of the OI sound reinforcement system denoted by t_{deb};

τ_u is a total duration of the violator's actions to intercept SEMR corresponding to the speeches of the event participants;

$\tau_u^{(1)}$, $\tau_u^{(2)}$, $\tau_u^{(3)}$ ... $\tau_u^{(N)}$ are durations of interception of SEMRs corresponding to the speeches of each participant of the event.

The impact of the used security measures on the possibility of intercepting voice information by SEMR is characterized as follows. If the violator detects a patrol group, then the equipment for intercepting the SEMR is turned off. In this case, the detection of a group can occur when the group arrives at the territory, during round and inspection by the group, during the deployment and configuration of the TM by the violator, as well as

during the interception of SEMR with voice information. At the same time, interception becomes impossible or the interception time is reduced and thus the ability of the violator to identify confidential information contained in the SEMR is reduced. If the violator does not detect the patrol group or ignores its actions, then with the activation of the mobile noise generator (or simulator), the interception of the SEMR is blocked, with the exception of the possibility of information leakage. Suppression can begin both during the existence of SEMR and before its appearance.

The use of the considered protection measures can significantly reduce the amount of intercepted information with a significant decrease in the semantic intelligibility of speech [20]. To ensure the specified intelligibility, the violator must intercept at least 25% of the amount of information (based on the required verbal intelligibility [7]).

The above ratios and conditions of interception are used in the mathematical model of the realizing the threat of interception of voice information by SEMR.

To assess the possibility of intercepting voice information by SEMR, it is proposed, by analogy with [18], to use a probabilistic indicator that is the probability of realizing the threat of interception of at least a given portion (δ_{sp}) of the volume of voice information of the n-th participant spoken during the time $\tau_{sp}^{(n)}$, $n = \overline{1, N}$ at this event.

At the same time, interception takes place under the following conditions. First, the following conditions are fulfilled: by the time the participant's speech containing confidential information begins to be intercepted, the sound reinforcement system was deployed and configured, the violator arrived at the territory adjacent to the protected area, deployed and tuned in the TM of the SEMR interception, and this was not detected by the RRT or suppressed by this group's mobile vehicle. Second, during the time $\tau_u^{(n)}$, the voice of the n-th participant of the event was intercepted by the SEMR.

The time of realization of the SEMR interception threat (t_u) is the sum of the times t_{terms} and τ_u. However, if the value t_{terms} can be considered to be exponentially distributed [21] with the mathematical expectation $\overline{t_{terms}}$, then the value $\tau_{sp}^{(n)}$ for the n-th participant is limited to the minimum $\tau_{sp\,n}^{\min}$ and the maximum $\tau_{sp\,n}^{\max}$ values and, in fact, has a uniform probability distribution. With accuracy sufficient for practice, the probability distribution for ($\tau_u^{(n)}$) can also be considered to be uniform. In this case, the following conditions must be fulfilled:

- the time required to form the conditions for interception of the SEMR by the violator (t_{terms}) should not exceed the time of waiting for the start of the event ($t_{sp}^{(1)}$);

- the total time $t_u^{(1)}$, which is required to form the conditions for interception of the SEMR and the interception itself, cannot be less than the sum of the time of waiting for the start of the event ($t_{sp}^{(1)}$) and the time required to intercept a given portion of the voice message ($\delta_{sp} \cdot \tau_{sp}^{(1)}$), which allows to reveal confidential information, but cannot exceed the total time of waiting for the start of the event and the time for the first participant at the event ($t_{sp}^{(1)} + \tau_{sp}^{(1)}$).

The quantity $t_u^{(1)}$ is the sum of the random variables t_{terms} distributed exponentially and $\tau_u^{(1)}$ distributed uniformly in the interval $\left[\tau_{u.\,\min}^{(1)}, \tau_{u.\,\max}^{(1)}\right]$. As the probability that the threat of voice information leakage by SEMR is realized during the speech of the first participant, the distribution function for such a sum is calculated by the formula

$$P_u^{(1)}(t) = \begin{cases} 0 \; pri, \; t \le a_1; \\ \left[\frac{t-a_1}{b_1-a_1} - \frac{1-e^{-\frac{(t-a_1)}{t_{terms}}}}{b_1-a_1} \cdot \overline{t_{terms}} \right] \quad pri \; a_1 < t < b_1; \\ \left[1 - \frac{1-e^{-\frac{(b_1-a_1)}{t_{terms}}}}{b_1-a_1} \cdot \overline{t_{terms}} \right] \quad pri \; t > b_1; \end{cases} \tag{1}$$

where $a_1 = t_{sp}^{(1)} + (1-\delta_{sp}) \cdot \tau_{u.\min}^{(1)}$ and $b_1 = t_{sp}^{(1)} + \tau_{u.\max}^{(1)}$.

If it is necessary to assess the possibility of information leakage by SEMR for the n-th participant (under the condition that the interception of the voice information of the previous $n-1$ participants took place), then similar conditions must be fulfilled as for the first participant. Wherein

$$t_{sp}^{(n-1)} = \sum_{k=1}^{n} \left(t_{sp}^{(k)} + \theta_k \right); \tag{2}$$

where

$t_{sp}^{(n-1)}$ is the time from the start of the event to the start of the performance of the n-th participant,

θ_k is the duration of the pause between the performances of the k-th and $(k+1)$-th participants.

Therefore, to calculate the probability of realizing the threat of information leakage by SEMR for n event participants, the same formulas are used, where the parameter $t_{sp}^{(1)}$ is replaced by the parameter $t_{sp}^{(n-1)}$.

For rough estimates, the probability that there is a leakage of voice information by SEMR for the period of the event for at least one participant is calculated by the formula:

$$P_u^{(n\ge 1)}(t) = 1 - \prod_{n=1}^{N} \left[1 - P_u^{(1)}(t) \right]. \tag{3}$$

To calculate the value $\overline{t_{terms}}$, we develop a mathematical model of the process of forming conditions for intercepting voice information by SEMR based on the apparatus of composite Petri – Markov nets.

3. Mathematical Model of the Process of Forming Conditions for Intercepting Voice Information by SEMR Based on the Apparatus of Composite Petri – Markov Nets

A descriptive model of the process of forming the conditions for intercepting voice information by the SEMR of the RED of the OI was used to form the Petri – Markov net (PMN) in the interests of modelling the dynamics of the implementation of this process. In this case, in accordance with [21], composite PMNs, which are Markov and semi-Markov partial processes combined through logical transitions, were used. Fig. 2 shows the PMN graph corresponding to the descriptive model of the process of forming the conditions for intercepting voice information by SEMR.

PMN includes a set of positions (numbered in order without letters and indices – 0, 1, 2, etc.) and a set of transitions (with numbers and the letter z – $0(z), 1(z), 2(z)$, etc.). Positions indicate the states of the modeled process at certain points in time, and transitions are actions that are implemented during the execution of the process.

The current state of the process is indicated by a label. To simulate a process of the type under consideration, a so-called ordinary network is used, in the initial state of which there is only one label.

The time of moving the process from position to transition is considered to be random and finite, and time of moving the process from transition to position is considered to be instantaneous. The directions of the label movement along the graph are indicated by arcs with arrows.

Transitions can be simple or logical. Simple transitions are triggered when a label arrives at them from an incident state, have one input and can have several outputs. Logical transitions have two or more inputs and are triggered when labels are received and when certain logical conditions are fulfilled.

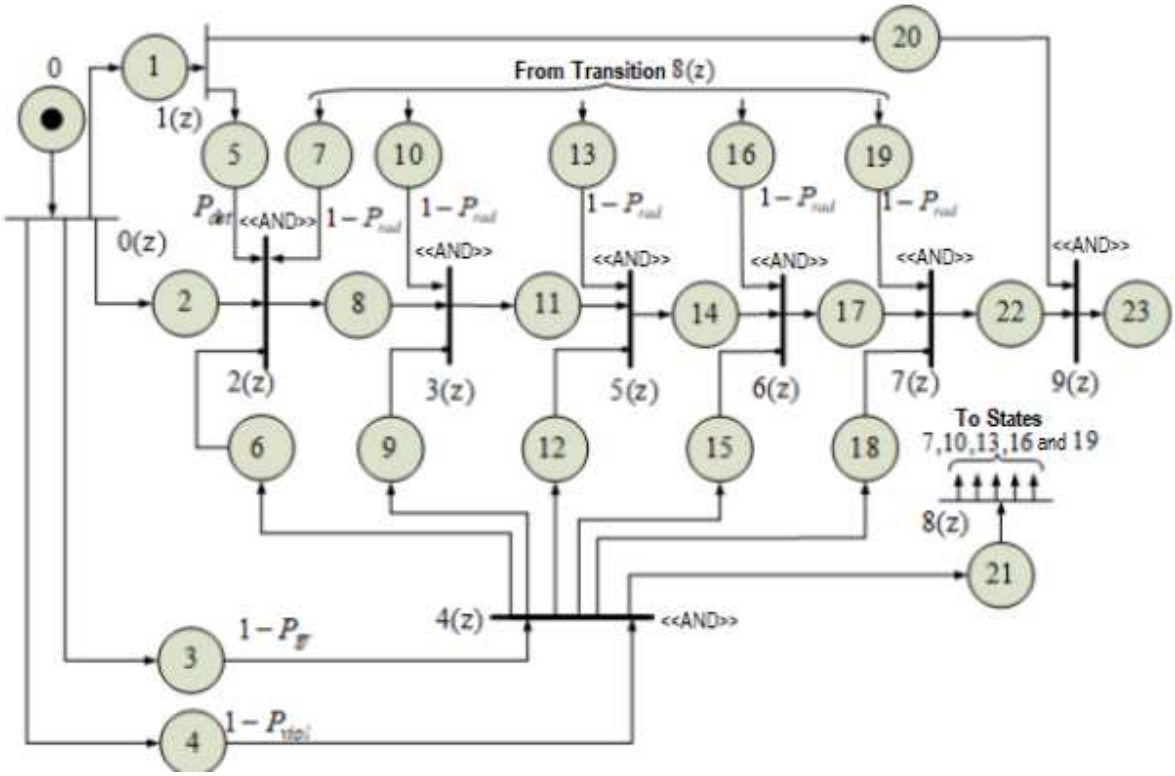

Fig. 2. The Petri – Markov network graph for the process of forming the conditions for the realization of the threat of interception of voice information by SEMR

In Fig. 2, we use the following notations.

For network positions:

0 stands for the initial state of the process: readiness for the event and the beginning of the deployment of the sound reinforcement system to support it, the RRT is ready to patrol the territory, the violator is ready to move to the territory adjacent to the protected area;

1 stands for the started testing and tuning the sound reinforcement system;

2 stands for the violator deployed the TM for intercepting SEMR and started scanning the frequency range to detect the SEMR;

3 stands for the RRT went out to patrol the territory adjacent to the CA to detect the violator;

4 stands for the violator started monitoring the territory to detect the RRT;

5 stands for the SEMR takes place during testing and tuning of the sound reinforcement system;

6, 9, 12, 15, 18 stand for the violator did not find the RRT on the territory (with the probability $1 - P_{viol}$) and the RRT did not find the violator (with the probability $1 - P_{gr}$);

P_{viol} is the probability of detecting a patrol group by a violator, $P_{viol} < 1$;

P_{gr} is the probability of detecting a violator by a patrol group, $P_{gr} < 1$;

7, 10, 13, 16, 19 stand for the noise generator was on, the suppression of the TM for interception of the SEMR was started with the probability P_{rad};

8 stands for SEMR was detected by the interceptor, determination of the direction of its maximum level was started;

11 stands for completion of Action 8 and start of finding the place from which the SEMR interception will be carried out;

14 stands for completion of Action 11 and start of determining the type of the SEMR signal and the spectrum width;

17 stands for completion of Action 14 and start of setting up the interception TM by the violator;

20 stands for completion of testing, the functioning of the sound reinforcement system is tuned and checked, the system is put into standby mode;

21 stands for the RRT deployed a mobile noise generator and received a command to suppress the violator's TM;

22 stands for completion of setting up the interception TM, the violator is ready to intercept the SEMR signal corresponding to the voice of the event participant;

23 stands for fulfillment of the conditions to implement the threat of interception of voice information of the event participant.

For network transitions, we use the following notations:

0 (z) stands for the violator moves through the territory adjacent to the CA, the RRT moves to patrol the territory;

1 (z) stands for start of testing, tuning and checking the functioning of the sound reinforcement system, the system is put into standby mode;

2 (z) stands for the logical transition "AND", which is triggered under the condition that the violator detected SEMR during the tuning of the sound reinforcement system while scanning the frequency range, and, at the same time, he did not detect the RRT (or ignored its appearance);

3 (z) stands for the logical transition "AND", which is triggered under the condition that the violator began to determine the maximum level of SEMR, but at the same time he did not detect the appearance of the RRT and the RRT did not detect the violator, and suppression of the interception TM did not exclude the reception of SEMR;

4 (z) stands for the logical transition "AND", which is triggered if the RRT did not detect the violator and the violator did not detect the RRT;

5 (z) stands for the logical transition "AND", which is triggered under the condition that the violator began to select a place for intercepting the SEMR during the setup of

the sound reinforcement system, but at the same time the violator did not detect the appearance of the RRT and the RRT did not detect the violator, and the suppression of the interception TM did not exclude the interception of SEMR;

6 (z) stands for the logical transition "AND", which is triggered under the condition that the violator began to determine the type of the SEMR signal and the spectrum width, but at the same time the violator did not detect the appearance of the RRT and the RRT did not detect the violator, and suppression of the interception TM did not exclude the interception of SEMR;

7 (z) stands for the logical transition "AND", which is triggered under the condition that the violator completed the configuration of the TM, while the violator did not detect the appearance of the RRT and the RRT did not detect the violator, and suppression of the interception TM did not exclude the interception of SEMR;

9 (z) stands for the logical transition "AND", which is triggered under the condition that the process approaches the transition along both arcs: both the sound reinforcement system and the intercept TM are configured.

For network arcs, we use the following notations:

an arc with an arrow indicates the direction of movement of the modeled process (for some arcs associated with the applied protection measures, the probability of movement along the arc is indicated);

an arc with a circle is a permissive arc: when the label arrives at the incident (outgoing) position, the transition to which such an arc approaches is allowed.

Taking into account the foregoing, the mathematical expectation ($\overline{t_{terms}}$) of the response time of the given PMN, that is, creating conditions for the implementation of the threat of interception of voice information by SEMR, is calculated as follows:

$$\overline{t_{terms}} = \overline{\tau_{0,0}} + \overline{\tau_{7(z)}} + \overline{\tau_{9(z)}}, \tag{4}$$

where $\overline{\tau_{9(z)}}$ is the average response time of the transition 9 (z).

Transitions 2 (z), 3 (z), 5 (z), 6 (z) and 7 (z) with the logical "AND" are triggered if the label approaches the transition along three arcs, which are two usual (with an arrow) arcs and a permissive one. Transitions 4 (z) and 9 (z) are triggered as ordinary transitions with the logical "AND" [21].

If the probability of moving along an usual arc is indicated, then the time increases in inverse proportion to this probability. For example, the average time of moving the process from State 1 to Transition 2 (z) is determined from the relation [22]

$$\overline{\tau_{1,2}} = \frac{\overline{\tau_{1,1}} + \overline{\tau_{5,2}}}{P_{\text{det}}}, \; P_{\text{det}} > 0, \tag{5}$$

where $\overline{\tau_{1,1}}$ and $\overline{\tau_{5,2}}$ are the average times for the process to move from State 1 to Transition 1 (z) and from State 5 to Transition 2 (z), respectively, when a SEMR is detected during the interception TM setup with the probability P_{det}.

Taking into account the above, the response times of logical transitions are calculated as follows [21].

For Transition 2 (z),

$$\overline{\tau_{2(z)}} = \frac{\overline{\tau_{2\wedge5\wedge7}}^2 + \overline{\tau_{2\wedge5\wedge7}} \cdot \overline{\tau_{4(z)}} + \overline{\tau_{4(z)}}^2}{\overline{\tau_{2\wedge5\wedge7}} + \overline{\tau_{4(z)}}}, \tag{6}$$

where $\overline{\tau_{2\wedge5\wedge7}}$ is an average time of the process moving to Transition 2 (z) and along the arc from State 2, and along the arc from State 5, and along the arc from State 7,

$$\overline{\tau_{2\wedge5\wedge7}} = \overline{\tau_{2,2}} + \frac{\overline{\tau_{5,2}}}{P_{\text{det}}} + \frac{\overline{\tau_{7,2}}}{1-P_{rad}} + \left(\frac{1}{\frac{1}{\overline{\tau_{2,2}}} + \frac{P_{\text{det}}}{\overline{\tau_{5,2}}}} + \frac{1}{\frac{1}{\overline{\tau_{2,2}}} + \frac{1-P_{rad}}{\overline{\tau_{7,2}}}} + \frac{1}{\frac{P_{\text{det}}}{\overline{\tau_{5,2}}} + \frac{1-P_{rad}}{\overline{\tau_{7,2}}}} \right) + \\ + \frac{1}{\frac{1}{\overline{\tau_{2,2}}} + \frac{P_{\text{det}}}{\overline{\tau_{5,2}}} + \frac{1-P_{rad}}{\overline{\tau_{7,2}}}}. \tag{7}$$

For Transition 3(z),

$$\overline{\tau_{3(z)}} = \overline{\tau_{2(z)}} + \frac{\overline{\tau_{8\wedge10}}^2 + \overline{\tau_{8\wedge10}} \cdot \overline{\tau_{4(z)}} + \overline{\tau_{4(z)}}^2}{\overline{\tau_{8\wedge10}} + \overline{\tau_{4(z)}}}, \tag{8}$$

where $\overline{\tau_{8\wedge10}}$ is an average time of the process moving to Transition 3 (z) from States 8 and 7,

$$\overline{\tau_{8\wedge10}} = \frac{\overline{\tau_{8,3}}^2 \cdot (1-P_{rad})^2 + \overline{\tau_{8,3}} \cdot \overline{\tau_{10,3}} \cdot (1-P_{rad}) + \overline{\tau_{10,3}}^2}{[\overline{\tau_{8,3}} \cdot (1-P_{rad}) + \overline{\tau_{10,3}}] \cdot (1-P_{rad})}. \tag{9}$$

For Transition 4(z),

$$\overline{\tau_{4(z)}} = \frac{\overline{\tau_{3,4}}^2 \cdot (1-P_{viol})^2 + \overline{\tau_{3,4}} \cdot \overline{\tau_{4,4}} \cdot (1-P_{gr}) \cdot (1-P_{viol}) + \overline{\tau_{4,4}}^2 \cdot (1-P_{gr})^2}{(1-P_{gr}) \cdot (1-P_{viol}) \cdot [\overline{\tau_{3,4}} \cdot (1-P_{viol}) + \overline{\tau_{4,4}} \cdot (1-P_{gr})]}. \tag{10}$$

For Transition 5(z),

$$\overline{\tau_{5(z)}} = \overline{\tau_{3(z)}} + \frac{\overline{\tau_{11\wedge13}}^2 + \overline{\tau_{11\wedge13}} \cdot \overline{\tau_{4(z)}} + \overline{\tau_{4(z)}}^2}{\overline{\tau_{11\wedge13}} + \overline{\tau_{4(z)}}}, \tag{11}$$

where $\overline{\tau_{11\wedge13}}$ is an average time of the process moving to Transition 5 (z) from States 11 and 13,

$$\overline{\tau_{11\wedge13}} = \frac{\overline{\tau_{11,5}}^2 \cdot (1-P_{rad})^2 + \overline{\tau_{11,5}} \cdot \overline{\tau_{13,5}} \cdot (1-P_{rad}) + \overline{\tau_{13,5}}^2}{[\overline{\tau_{11,5}} \cdot (1-P_{rad}) + \overline{\tau_{13,5}}] \cdot (1-P_{rad})}. \tag{12}$$

For Transition 6(z),

$$\overline{\tau_{6(z)}} = \overline{\tau_{5(z)}} + \frac{\overline{\tau_{14\wedge16}}^2 + \overline{\tau_{14\wedge16}} \cdot \overline{\tau_{4(z)}} + \overline{\tau_{4(z)}}^2}{\overline{\tau_{14\wedge16}} + \overline{\tau_{4(z)}}}, \tag{13}$$

where $\overline{\tau_{14\wedge16}}$ is an average time of the process moving to Transition 6 (z) from States 14 and 16,

$$\overline{\tau_{14\wedge16}} = \frac{\overline{\tau_{14,6}}^2 \cdot (1-P_{rad})^2 + \overline{\tau_{14,6}} \cdot \overline{\tau_{16,6}} \cdot (1-P_{rad}) + \overline{\tau_{16,6}}^2}{[\overline{\tau_{14,6}} \cdot (1-P_{rad}) + \overline{\tau_{16,6}}] \cdot (1-P_{rad})}. \tag{14}$$

For Transition 7(z),

$$\overline{\tau_{7(z)}} = \overline{\tau_{6(z)}} + \frac{\overline{\tau_{17\wedge19}}^{22} + \overline{\tau_{17\wedge19}} \cdot \overline{\tau_{4(z)}} + \overline{\tau_{4(z)}}^2}{\overline{\tau_{17\wedge19}} + \overline{\tau_{4(z)}}}, \tag{15}$$

where $\overline{\tau_{17\wedge19}}$ is an average time of the process moving to Transition 7 (z) from States 17 and 19,

$$\overline{\tau_{17\wedge19}} = \frac{\overline{\tau_{17,7}}^2 \cdot (1 - P_{rad})^2 + \overline{\tau_{17,7}} \cdot \overline{\tau_{19,7}} \cdot (1 - P_{rad}) + \overline{\tau_{19,7}}^2}{[\overline{\tau_{17,7}} \cdot (1 - P_{rad}) + \overline{\tau_{19,7}}] \cdot (1 - P_{rad})}. \tag{16}$$

For Transition 9(z),

$$\overline{\tau_{9(z)}} = \frac{\overline{\tau_{22,9}}^2 + \overline{\tau_{22,9}} \cdot \overline{\tau_{20,9}} + \overline{\tau_{20,9}}^{22}}{\overline{\tau_{22,9}} + \overline{\tau_{20,9}}}. \tag{17}$$

The dynamics of the implementation of protection measures against interception of voice information by SEMR is taken into account by the parameter $\overline{t_{terms}}$ in accordance with relations (5) - (17) and the probabilities P_{gr}, P_{viol}, P_{det} and P_{rad}, when formula (4) is used to calculate the expectation of the time of creating conditions to realize the threat of such interception. If it is necessary to assess the possibility of intercepting the speechs of several participants in the event, then the times of their speechs (taking into account the pauses between them) are summed up. In this case, to quantify the protection of voice information from leakage, formulas (1) and (3) are used.

4. Experiment Results

To check the adequacy of the developed models and the correctness of the obtained assessments of the protection of voice information against leakage due to SEMR of the RED of the OI, experimental studies were carried out in the form of a computational experiment. In the course of the experiment, we set the values of time parameters characterizing the actions of the violator, the processes of interception of voice information by SEMR and the application of protective measures:

$\overline{\tau_{0,0}}$ is an average time before the start of the first participant's performance (that corresponds to the time $\overline{t_{sp}}$) and equals to 5 min;

$\overline{\tau_{1,1}}$ is an average time to turn on and prepare the sound reinforcement system for testing and tuning and equals to 3 min;

$\overline{\tau_{2,2}}$ is an average time of scanning the frequency range by the violator and equals to 5 min;

$\overline{\tau_{3,4}}$ is an average time for a patrol group to search for a violator and equals to 7 min;

$\overline{\tau_{4,4}}$ is an average time of detection of a patrol group by a violator and equals to 2 min;

$\overline{\tau_{5,2}}$ is an average time of SEMR detection during testing and tuning of the sound reinforcement system and equals to 2 min;

$\overline{\tau_{6,2}}$, $\overline{\tau_{9,3}}$, $\overline{\tau_{12,5}}$, $\overline{\tau_{15,6}}$, $\overline{\tau_{18,7}}$ is an average time of accounting for conditions and equals to 0 min;

$\overline{\tau_{7,2}}$, $\overline{\tau_{10,3}}$, $\overline{\tau_{13,5}}$, $\overline{\tau_{16,6}}$, $\overline{\tau_{19,7}}$ is an average time without suppression of the interception TM during tuning of the sound reinforcement system, the determining the direction of the maximum level of SEMR radiation, the choice of the place from which the SEMR interception should be carried out, the determining the signal type and the width of its spectrum, the setting of the TM of the SEMR interception, and equals to 2, 2, 5, 3, 2 min, respectively;

$\overline{\tau_{8,3}}$ is an average time to determine the direction of the maximum SEMR radiation level and equals to 1 min;

$\overline{\tau_{11,5}}$ is an average time of choosing the place from which the SEMR should be intercepted and equals to 5 min;
$\overline{\tau_{21,8}}$ is an average time of noise generator deployment and equals to 0.5 min;
$\overline{\tau_{14,6}}$ is an average time to determine the type of the SEMR signal and the width of its spectrum and equals to 2 min;
$\overline{\tau_{17,7}}$ is an average time for a violator to set up a TM to intercept and equals to 2 min;
$\overline{\tau_{20,9}}$ is a report on readiness and switching the sound reinforcement system to standby mode and equals to 0.1 min;
$\overline{\tau_{22,9}}$ is a waiting for the start time of the participant's performances and equals to 2 min.

We assume that the violator arrived at the start of the preparation for the event.

The formation of the initial data was carried out taking into account the terrain conditions of the territory adjacent to the CA of the object located at a distance of 30 m from the park zone, and the characteristics of the interception TM. The length of the territory along the CA of the OI is 200 m, and the width is 30 m.

As an interception TM, we use an AR-8200 receiver with the following characteristics: frequency range is 0.5 – 2040 MHz; scanning speed is up to 37 frequencies (channels) per second (at a scanning step of 100 kHz, the frequency range is scanned in 9 min); types of signal modulation are AM, FM; sensitivity is 0.7 – 3.5 microvolt and 0.5 - 2.5 microvolt in AM mode and in FM mode, respectively [23].

The OI sound reinforcement system includes: 23 T-621 A microphones; mixer BEHVINGER SX 3242 FX; amplifier ROXTON AA-240; 6 loudspeakers INTER M; connecting lines (twisted pair) from microphones to a mixer with a length of 10 – 40 m; connecting lines (twisted pair) from the mixer to the amplifier with a length of 0.1 – 0.2 m; connecting lines (twisted pair) from the amplifier to the loudspeakers with a length of 10 – 30 m.

The ISS, which implements protection measures during the experiment, includes the following elements.

1. Video surveillance system consists of video cameras Axis, software is Axis camera station; Unifi video cameras, web interface is Unifi Video; Intel Celeron computer with control and video processing modules (1.3 GHz, 2 GB of RAM), Microsoft Windows XP.

2. Three RRTs consist of three patrol officers, each of which is equipped with technical means of information protection: a mobile radio noise generator of the "SHTORA" series to protect against information leakage due to SEMR, which arose during the operation of electronic means of processing, storage and transmission of information (operating frequency range is 0.1 – 2500 MHz; increased output power is up to 35 W; battery life is up to 50 min).

3. The video cameras are controlled by the security administrator through a server located in the local network of the organization. Each camera has its own local address. The RRT patrols carry out patrol in accordance with the administrator's commands.

Results of calculating the time parameters of logical network transitions and the mathematical expectation of the time of creating conditions for intercepting SEMR for two variants of the initial values of the probabilities P_{det}, P_{gr}, P_{viol} and P_{rad} for $\delta_{sp} = 0.25$, $\tau^{(1)}_{u.\,\min} = 7$ min , $\tau^{(1)}_{u.\max} = 15$ min are shown in Table 1, and Figs. 3 and 4 show the graphs of the dependence of the interception probability on time calculated by formulas (3) for one participant and for the specified options obtained using the Mathcad programm.

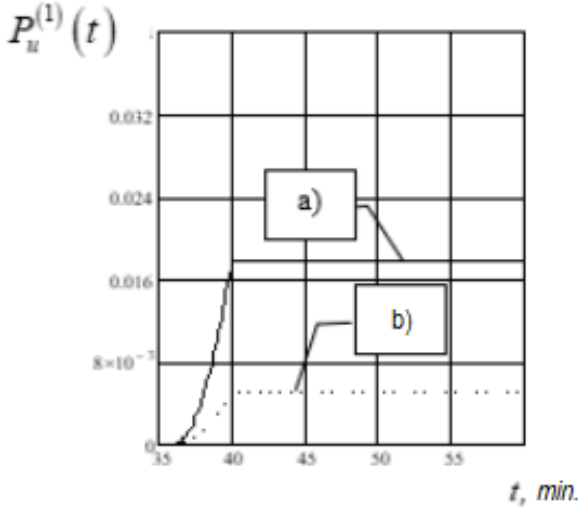

Fig. 3. Graph of the dependence of the probability to realize the threat of voice information leakage on time for the first of the event participants for variants a) and b) of the initial data (Table 1)

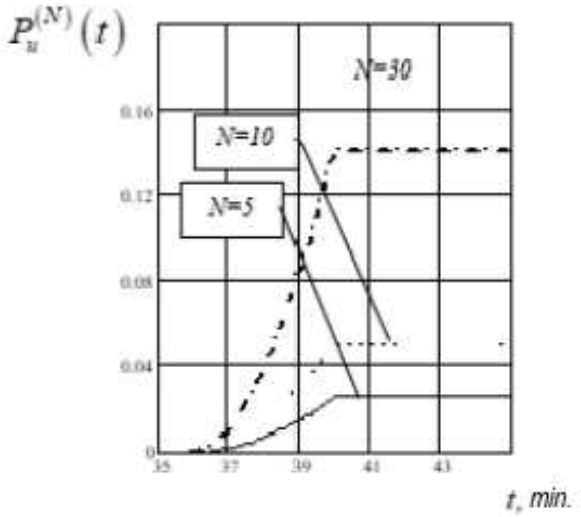

Fig. 4. Graph of the dependence of the probability to realize the threat of voice information leakage on time for at least one of N participants of the event for variant b) of the initial data (Table 1)

Table 1

Results of calculating the response times of logical transitions and the Petri – Markov net as a whole

Parameter	Parameter value, min.	Parameter	Parameter value, min.
Variant a): $P_{gr} \approx 0.9$, $P_{viol} \approx 0.9$, $P_{\text{det}} \approx 0.1$, $P_{rad} = 0.9$ (almost no protection)		Variant b): $P_{gr} = 0.5$, $P_{viol} = 0.5$, $P_{\text{det}} = 0.3$, $P_{rad} = 0.1$	
$\overline{\tau_{2(z)}}$	67	$\overline{\tau_{2(z)}}$	86
$\overline{\tau_{3(z)}}$	75	$\overline{\tau_{3(z)}}$	70
$\overline{\tau_{4(z)}}$	7	$\overline{\tau_{4(z)}}$	74
$\overline{\tau_{5(z)}}$	85	$\overline{\tau_{5(z)}}$	240
$\overline{\tau_{6(z)}}$	94	$\overline{\tau_{6(z)}}$	316
$\overline{\tau_{7(z)}}$	103	$\overline{\tau_{7(z)}}$	386
$\overline{\tau_{9(z)}}$	1.5	$\overline{\tau_{9(z)}}$	1.5
$\overline{t_{terms}}$	110	$\overline{t_{terms}}$	392

The possibilities of intercepting SEMR for voice information of at least one of several participants in the event increase significantly with the increase in the number of participants (or the total duration of the event). For example, for 30 participants in comparison with 5 participants, the probability of voice information leakage by SEMR increases almost 6 times and reaches 0.14.

Fig. 5 shows the dependence of the probability to intercept the SEMR on the

probability of their detection by the violator during the setup of the interception TM for the first participant and for 20 participants of the event, and Fig. 6 presents the dependence of the probability to intercept the SEMR on the probability of detection of a violator by a patrol group on the territory with subsequent expulsion of the violator in the absence of other protection measures.

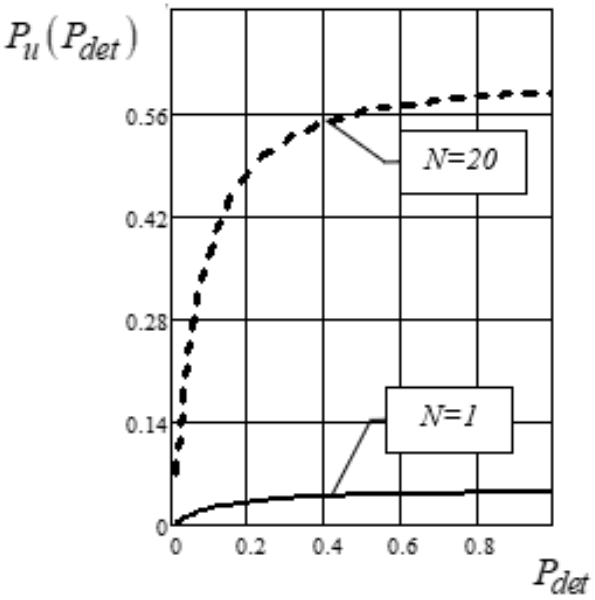

Fig. 5. Graph of dependence of the probability to realize the threat of voice information leakage for the first participant on the probability of detecting SEMR during the setup of the sound reinforcement system and the interception TM

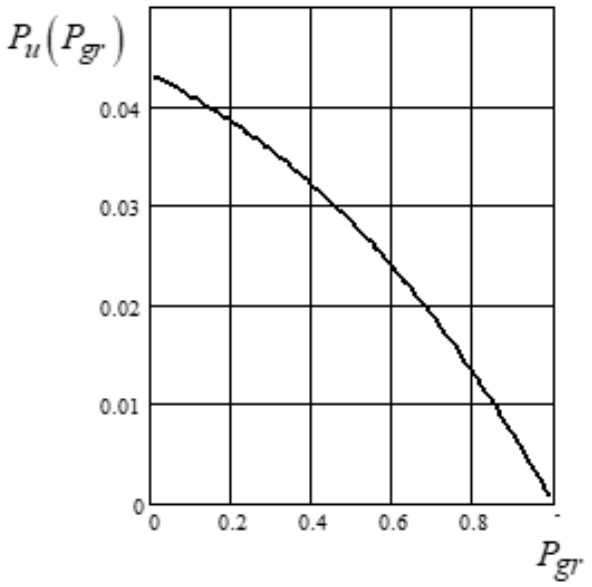

Fig. 6. Graph of the dependence of the probability to realize the threat of voice information leakage on the probability of detecting the violator and expulsion of the violator from the territory adjacent to the protected one

The analysis of the obtained results of the computational experiment showed the following.

1. The possibilities of intercepting voice information by SEMR, even under ideal conditions for their detection in the energy sector, turn out to be very small if the speech duration does not exceed 10-15 minutes, even in the absence of protective measures such as searching for and expulsion of the violator from the territory adjacent to CA, immediately before and during the event. Therefore, when analyzing the protection of voice information against leakage by SEMR, it is necessary to assess not only the possibility of detecting SEMR by its spectral power density, but also the possibility of intercepting SEMR in time.

2. With an increase in the duration of a participant's speech containing confidential information, or the need to protect information during the entire event as a whole, the possibility of intercepting SEMR in time increases significantly without the use of adequate protection measures. The developed model of the analysis of these possibilities based on the apparatus of the Petri – Markov nets allows for the first time to take into account the time factor when justifying the timing of the application of measures for the protection of voice information when planning and carrying out events of a confidential nature.

Conclusion

The traditional approach to assessing the indicators of the security of voice information against leakage due to SEMR of the RED of the OI on the basis of instrumental and calculation methods under the conditions of the dynamics of the implementation of the interception process by the violator turns out to be incomplete. The lack of taking into account the time factor does not allow the correct justification of the timing of the application of measures of protection against threats of interception of voice information by SEMR that are not related to the energy capabilities of their detection.

To take into account the time factor when assessing the possibility of intercepting SEMR of the RED of the OI, we propose a mathematical model developed on the basis of the apparatus of Petri – Markov nets, and obtain relations for calculating the indicator of information protection against leakage due to SEMR, which allows to take into account the effect of protection measures on the possibility of such a leakage.

This makes it possible to quantitatively substantiate the requirements for the time characteristics of the implementation of information protection measures and, above all, measures of an organizational and technical nature within the framework of protection systems.

In this subject area, promising areas for further research are as follows:

1) development of analytical models to calculate indicators for assessing the possibility of detecting a violator on the territory by a patrol group in time and the influence of the probabilities of suppression of interception TM on the possibility of intercepting voice information, taking into account the statistical time characteristics of the process of conducting confidential events (duration, number and duration of speeches, etc.);

2) conducting theoretical and experimental studies on the standardization of the values of information protection indicators against leakage due to SEMR of the RED of the OI in the interests of substantiating the requirements for the time characteristics of the ISS response to the actions of the violator and the implementation of preventive measures to protect information;

3) development of software tools for automating the assessment of information protection against leakage due to the SEMR of the RED of the OI in the context of the dynamics of the violator's implementation of interception and the application of preventive protection measures.

References

1. [*ISO/IEC 15408-3-2008. Information Technology. Security Techniques. Evaluation Criteria for IT Security. Part 3: Security Assurance Components*], 2008.
2. [*ISO/IEC 15408-1-2017. Information Technology. Security Techniques. Evaluation Criteria for IT Security. Part 1: Introduction and General Model*], 2017.
3. Avdeev V. B., Kartusha A. N. Calculation of Stray Electromagnetic Radiation Attenuation factor. *Special Equipment*, 2013, no. 2. pp. 18–27. (in Russian)
4. Avdeev V. B., Anishchenko A. V., Petigin A. F. Methodological Approach to Protection of Information to be Computer Processed with tre Use of Complex Signals, against the Leakage due to Stray Electromagnetic Radiation. *Special Equipment*, 2017, no. 3. pp. 40–47. (in Russian)

5. Antipov D. A., Shelupanov A. A. Research of the Direction of Secondary Electromagnetic Radiation from a Personal Computer. *Proceedings of TUSUR*, 2018, vol. 21, no. 2. pp. 33—37. DOI: 10.21293/1818-0442-2018-21-2-33-37. (in Russian)
6. Ismibeyli E. *Electrodynamics and Propagation of Radio Waves. Workbook for Universities*. LAP Lambert Academic Publishing, 2014.
7. Khorev A. A. Monitoring Systems to Detection of Audio Surveillance Equipment. *Protection of Information. Inside*, 2018, no. 1 (79), pp. 14—31. (in Russian)
8. Zaitsev A. P., Shelupanov A. A., Meshcheryakov R. V. [*Technical Means and Methods of Information Protection: a Textbook for Universities*]. Moscow, Goryachaya Liniya – Telekom Publ., 2012. (in Russian)
9. Skryl' S. V., Nikulin S. S., Ponomarev M. V., Tegentsev I. M., Kuznetsov M. V. Expert Approach to Assessment of Level of Threat of Information Leakage on Pemin Channels and her Security from Such Threats. *Industrial ACS and Controllers*, 2018, no. 4. pp. 45–53. (in Russian)
10. Sychev M. P., Skryl S. V., Nikulin S. S., Shcherbakov A. V., Spivak V. I. Functional Model of Place Search Process of Signal Reconnaissance-Availability of Side Electromagnetic Radiations and Pickups Modulated by Informative Signals. *Telecommunications*, 2019, no. 6. pp. 28–32. (in Russian)
11. 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. DOI: 10.1007/s00236-018-0320-2.
12. 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. *Proceedings of the Tenth International Conference on Management Science and Engineering Management*, 2017, vol. 502, pp. 913–920. DOI: 10.1007/978-981-10-1837-4_76.
13. Stetsenko I. V., Dyfuchyna O. Simulation of Multithreaded Algorithms using Petri-Object Models. *Advances in Computer Science for Engineering and Education*, 2019, vol. 754, pp. 391–401. DOI: 10.1007/978-3-319-91008-6_39.
14. Karyotis V., Khouzani M. H. R. *Malware Diffusion Models for Wireless Complex Networks. Theory and Applications*. Elsevier Inc., 2015. DOI: 10.1016/C2014-0-02168-5.
15. 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, issue 7, pp. 1319–1337. DOI: 10.1080/03610926.2013.768666.
16. 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, Jun 2012*. Helsinki, Finland, 2012, pp. 6073–6082.
17. Yang M., Wang M., Qu Y. Modeling and Performance Analysis of the Emergency Rescue Logistics System Based on Petri Nets. *Journal of Hebei University of Science and Technology*, 2017, vol. 38, no. 3, pp. 269–277. DOI: 10.7535/hbkd.2017yx03009.

18. Yazov Yu. K., Avsentiev O. S., Avsentev A. O., Rubtsova I. O. Method for Assessing Effectiveness of Protection of Electronic Document Management Using the Petri and Markov Nets Apparatus. *Tr. SPIIRAN*, 2019, vol. 18, no. 6, pp. 1269–1300. DOI: 10.15622/sp.2019.18.6.1269-1300. (in Russian)
19. Avsentev A. O., Krugov A. G., Perova Yu. P. Functional Models of Information Protection Against Leakage Due to Spurious Electromagnetic Emissions of Informatization Objects. *Proceedings of TUSUR University*, 2020, vol. 23, no. 2, pp. 17–35. DOI: 10.21293/1818-0442-2020-23-2-17-35. (in Russian)
20. Yamamoto K., Nakagawa S. Privacy Protection for Speech Information. *2009 Fifth International Conference on Information Assurance and Security, 18–20 Aug. 2009*, 2009, vol. 5, pp. 284–292. DOI: 10.1109/IAS.2009.321.
21. Yazov Yu. K., Anischenko A. V. [*Petri – Markov Nets and Their Application for Modeling the Processes of Implementation of Threats to Information Security in Information Systems*]. Voronezh, Kvarta Publ., 2020. (in Russian)
22. Klimov G. P. [*Stochastic Queueing Systems*]. Moscow, Nauka Publ., 1966. (in Russian)
23. [*Scanning Receiver AR8200. Operation Manual*], available at: https://docplayer.ru/32659500-Skaniruyushchiy-priemnik-ar8200-instrukciya-po-ekspluatacii-1-soderzhanie.html (accessed on October 12, 2020). (in Russian)

Oleg S. Avsentev, DSc (Techn), Full Professor, Professor at the Department of Information Security, Voronezh Institute of the Ministry of the Interior of the Russian Federation (Voronezh, Russian Federation), osaos@mail.ru.

Alexander O. Avsentev, PhD (Techn), Senior Lecturer at the Department of Physics and Radio Electronics, Voronezh Institute of the Ministry of the Interior of the Russian Federation (Voronezh, Russian Federation), aoaao8787@mail.ru.

Artem G. Krugov, Deputy Head of the Department for Organization of Implementation and Operation of Technical Means of Protection and Security of the Directorate of Non-Departmental Security of the National Guard Troops in the Tver Region (Tver, Russian Federation), krtemik@gmail.com.

Yurii K. Yazov, DSc (Techn), Full Professor, Professor at the Department of Systems of Information Security, Voronezh State Technical University (Voronezh, Russian Federation), yazoff_1946@mail.ru.

Received May 21, 2021.

УДК 621.3 DOI: 10.14529/jcem210201

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ОТ УТЕЧКИ ПО КАНАЛАМ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ С ПРИМЕНЕНИЕ АППАРАТА СЕТЕЙ ПЕТРИ – МАРКОВА

О. С. Авсентьев, А. О. Авсентьев, А. Г. Кругов, Ю. К. Язов

В статье предложено для количественной оценки защищенности информации на объектах информатизации (ОИ) от утечки по каналам побочных электромагнитных излучений (ПЭМИ) моделировать процессы перехвата ПЭМИ с применением аппарата сетей Петри-Маркова, позволяющего учитывать вероятностно-временные характеристики параллельно реализуемых процессов перехвата таких излучений, возникающих в радиоэлектронных устройствах (РЭУ) структурных элементов (СЭ) объекта, действий нарушителя, реализующего перехват из-за пределов контролируемой зоны (КЗ), а также меры защиты, направленные на пресечение возможности перехвата ПЭМИ. Полагается, что энергетические и частотные характеристики ПЭМИ, позволяют нарушителю в отсутствии мер защиты осуществлять такой перехват. Приведены показатели оценки и получены аналитические зависимости для их расчета. Модель позволяет оценить возможность перехвата во времени информации, относящейся к конфиденциальной, а также влияние мер защиты на возможности нарушителя по перехвату ПЭМИ, содержащих сведения конфиденциального характера. Приведены примеры расчета предложенных показателей при анализе защищенности речевой информации от перехвата по ПЭМИ РЭУ ОИ, оценено влияние превентивных организационных и технических мер защиты на снижение возможностей перехвата в зависимости от оперативности и сроков их проведения. На основе проведенного вычислительного эксперимента показана необходимость при анализе защищенности речевой информации от утечки по ПЭМИ оценивать не только возможности энергетического обнаружения ПЭМИ, но и возможности перехвата ПЭМИ во времени.

Ключевые слова: показатель защищенности информации; побочные электромагнитные излучения; сеть Петри-Маркова; превентивные меры защиты информации; технический канал утечки информации; временные характеристики.

Литература

1. ИСО/МЭК 15408-3-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности. – 2008.
2. ИСО/МЭК 15408-1-2017. Информационные технологии Методы и средства обеспечения безопасности Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель. – 2017.
3. Авдеев, В. Б. Расччт коэффициента ослабления побочных электромагнитных излучений / В. Б. Авдеев, А. Н. Катруша // Специальная техника. – 2013. – № 2. – С. 18–27.
4. Авдеев, В. Б. Методический подход к оценке защищчнности информации, обрабатываемой компьютером с использованием сложных сигналов, от утечки за сччт побочных электромагнитных излучений / В. Б. Авдеев, А. В. Анищенко, А. Ф. Петигин // Специальная техника. – 2017. – № 3. – С. 40–47.

5. Антипов, Д. А. Исследование направленности побочного электромагнитного излучения от персонального компьютера / Д. А. Антипов, А. А. Шелупанов // Доклады ТУСУР. – 2018. – Т. 21, № 2. – С. 33–37.

6. Ismibeyli, E. Electrodynamics and Propagation of Radio Waves. Workbook for Universities / E. Ismibeyli. – LAP Lambert Academic Publishing, 2014.

7. Хорев, А. А. ПАК для выявления электронных устройств перехвата речевой информации / А. А. Хорев // Защита информации. Инсайд. – 2018. – № 1 (79). – С. 14–31.

8. Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков. – М.: Горячая линия – Телеком, 2012.

9. Скрыль, С. В. Экспертный подход к оценке уровня угрозы утечки информации по каналам ПЭМИН и ее защищенности от такого рода угроз / С. В. Скрыль, С. С. Никулин, М. В. Пономарчв, И. М. Тегенцев, М. В. Кузнецов // Промышленные АСУ и контроллеры. – 2018. – № 4. – С. 45–53.

10. Сычев, М. П. Функциональная модель процесса поиска мест разведдоступности сигналов побочных электромагнитных излучений и наводок, модулированных информативными сигналами / М. П. Сычев, С. В. Скрыль, С. С. Никулин, А. В. Щербаков, В. И. Спивак // Телекоммуникации. – 2019. – № 6. – С. 28–32.

11. 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.

12. 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 // Proceedings of the Tenth International Conference on Management Science and Engineering Management. – 2017. – V. 502. – P. 913–920.

13. Stetsenko, I. V. Simulation of Multithreaded Algorithms using Petri-Object Models / I. V. Stetsenko, O. Dyfuchyna // Advances in Computer Science for Engineering and Education. – 2019. – V. 754. – P. 391–401.

14. Karyotis, V. Malware Diffusion Models for Wireless Complex Networks. Theory and Applications / V. Karyotis, M. H. R. Khouzani. – Elsevier Inc, 2015.

15. 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, iss. 7. – P. 1319–1337.

16. 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, Jun 2012. – Helsinki, Finland, 2012. – P. 6073–6082.

17. Yang, M. Modeling and Performance Analysis of the Emergency Rescue Logistics System Based on Petri Nets / M. Yang, M. Wang, Y. Qu // Journal of Hebei University of Science and Technology. – 2017. – V. 38, № 3. – P. 269–277.

18. Язов, Ю. К. Метод оценивания эффективности защиты электронного документооборота с применением аппарата сетей Петри – Маркова / Ю. К. Язов, О. С. Авсентьев, А. О. Авсентьев, И. О. Рубцова // Труды СПИИРАН. – 2019. – Т. 18, № 6. – С. 1269–1300.
19. 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. 17–35.
20. Yamamoto, K. Privacy Protection for Speech Information / K. Yamamoto, S. Nakagawa // 2009 Fifth International Conference on Information Assurance and Security, 18–20 Aug. 2009. – 2009. – V. 5. – P. 284–292.
21. 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.
22. Климов, Г. П. Стохастические системы массового обслуживания. – М.: Наука, 1966.
23. Сканирующий приемник AR8200. Инструкция по эксплуатации [Электронный ресурс]. – URL: https://docplayer.ru/32659500-Skaniruyushchiy-priemnik-ar8200-instrukciya-po-ekspluatacii-1-soderzhanie.html (дата обращения: 12.10.2020).

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

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

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

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

Поступила в редакцию 21 мая 2021 г.