Increasing the energy efficiency of electronic document management systems

Sergey Belokurov[1 *], *Alexei* Skrypnikov[1], *Oleg* Kondratov[1], *Dmitry* Levushkin[1] and *Oleg* Tveritnev[2]

[1] State University of Engineering Technologies, Faculty of Management and Informatics in Technological Systems, 19 Revolyutsii Avenue, Voronezh, Russia
[2] Mytishchi branch Bauman Moscow State Technical University, Faculty of Forestry, Mytishchi, ul. 1-ya Institutskaya, 1, Moscow Region, Russia

Abstract. This paper proposes a comprehensive set of characteristics of integrated security systems of electronic document management. We give a classification description and data analysis for modeling decision-making processes in integrated security systems by the example of responding to the threats of information leakage through parametric channels. The optimal set of measures to respond to an attacker's operations of illegal interception of information via parametric channels by using the appropriate modes of operation of the TCP protocol, which reduces the decision-making time, optimizes the performance of the system as a whole and significantly contributes to the optimization of its energy efficiency is given.

1 Introduction

Electronic document management systems in today's realities, including pandemic and remote access to information resources are among the most demanded and critical in terms of security integrated security systems (ISS). This article proposes a comprehensive set of characteristics of such ISB, which allows to conduct research on the degree of protection of such systems from external and internal threats from the perspective of system analysis and to model their functioning in different conditions. Let us define a set of mathematical models to assess the characteristics of the effectiveness of response measures to threats of information leakage through parametric channels [1-4].

2 Materials and methods

In accordance with the compositional nature of the procedure for forming a system of characteristics of the effectiveness of response measures to threats of information leakage through parametric channels, the input data for mathematical models of characteristics of the second level of the hierarchy of such a system are the values of the characteristics of the first (lower) level:

* Corresponding author: bsvlabs@mail.ru

- set $\{\omega(oijk)\}$ of temporal characteristics of operations of illegal actions for interception of information via parametric channels;

- set $\{\tau(vijk)\}$ of temporal characteristics of the functions for detecting signs of illegal actions of an intruder to intercept information via parametric channels;

The characteristics $\{\omega(oijk)\}$ and $\{\tau(vijk)\}$ are set empirically and are random variables [8-10].

Characteristics of the second level of the system of characteristics of the effectiveness of response measures to threats of information leakage through parametric channels are evaluated by the following sets of models:

- a set of models $\{M(\overline{\omega}\ (pjk))\}$ to estimate the average values of the implementation times of the TCP modes during illegal actions for interception of information via parametric channels;

- a set of models $\{M(\overline{\tau}\ (yjk))\}$ to estimate the average values of time to establish the facts of the implementation of certain modes of TCP during illegal actions for interception of information via parametric channels.

Characteristics of the third level of the system of characteristics of the effectiveness of response measures to threats of information leakage through parametric channels are evaluated by the following sets of models:

- a set of models $\{M(\overline{\omega}\ (ek))\}$ to estimate the average values of time of implementation by an attacker of individual stages of illegal actions to intercept information via parametric channels;

- a set of models $\{M(\overline{\tau}\ (ek))\}$ to estimate the average response time to the actions of the attacker during the implementation of individual stages of illegal actions to intercept information via parametric channels;

- set of models $\{M(P_{(p)k})\}$ to estimate the probabilities of timely response to the actions of the attacker when he implements the individual stages of illegal actions to intercept information via parametric channels.

Assessment of the characteristic of the fourth level - system indicator R of timeliness of response to threats of information leakage through parametric channels is carried out under the assumption of independence of events related to timely response to actions of intruder during implementation by him of separate stages of illegal actions of information interception through parametric channels.

Temporal characteristics of the intruder's ability to implement modes of operation of the TCR in the process of illegal actions for interception of information via parametric channels are formed at the second composite level of the system of characteristics of effectiveness of response measures to this kind of threats to information security [11, 12]. The formation procedure is based on the establishment of interlevel composite links of these characteristics with the characteristics of the initial (first) level of this system. The content of these links, and, consequently, the type of mathematical models of characteristics of this level is determined by the relevant functional models of illegal actions to intercept information via parametric channels. Typical formats of formed analytical dependencies are presented in [8-10].

The following expressions (1) - (15) are mathematical models for estimation of average values of time of realization of operation modes of TCP during illegal actions on interception of information via parametric channels. In accordance with the order of operations, given in [1, 4], performed by an intruder in the process of configuration of AP equipment through the channels of acousto-electrical transformations, HF irradiation, parasitic (auto) generation and HF imposition, the average value $\overline{\omega}\ (p11)$ of the random value of time, spent by an intruder on the realization of this mode of TCR operation is determined in accordance with the expression:

$$\overline{\omega}\ (p11) = \overline{\omega}\ (o111) + \overline{\omega}\ (o112) + \rho_{113}(\cdot E(\omega(o113)\ \omega(o115)) + \rho_{114(}\cdot o114\,\overline{\omega}\ ) + \\ + \rho_{116(}\cdot o116\,\overline{\omega}\ ) + \rho_{117(}\cdot o117\,\overline{\omega}\ ), \quad (1)$$

where ρ_{113}, ρ_{114}, ρ_{116} and ρ_{117} are the probabilities of performing operations *o113*, *o114*, *o116* and ρ_{o117} by the intruder in the process of illegal actions, respectively, $\overline{\omega}$ (*o111*), $\overline{\omega}$ (*o112*), $\overline{\omega}$ (*o114*), $\overline{\omega}$ (*o116*) and $\overline{\omega}$ (*o117*) are the mean values of random values of time spent by the attacker to perform operations *o111*, *o112*, *o114*, *o116*, and *o117*, respectively, and $E(\omega(o113)\omega^{\circ}(o115))$ means the mean value of the composition of the random variables $\omega(o113)$ and $\omega(o115)$ of the time the attacker performed operations *o113* and *o115*, respectively.

The order in which an intruder performs operations in the process of locating sources of informative acoustic signals of the reconnaissance object allows to form an expression to determine the average value $\overline{\omega}$ (*p12*) of the random value of time spent by the intruder on the implementation of this mode of operation:

$$\overline{\omega}(p12) = \overline{\omega}(o121) + \overline{\omega}(o122) + \rho_{123}(\cdot o123\,\overline{\omega}) + \rho_{124}(\cdot o124\,\overline{\omega}) + \\ + \rho_{125}\,\overline{\omega}(\cdot o125) + \rho_{126}\,\overline{\omega}(\cdot o126), \quad (2)$$

where ρ_{123}, ρ_{124}, ρ_{125} and ρ_{126} are the probabilities of performing operations *o123*, *o124*, *o125* and ρ_{126}, respectively, $\overline{\omega}$ (*o121*), $\overline{\omega}$ (*o122*), $\overline{\omega}$ (*o123*), $\overline{\omega}$ (*o124*), $\overline{\omega}$ (*o125*) and $\overline{\omega}$ (*o126*) are the average random values of time spent by the intruder to perform operations *o121*, *o122*, *o123*, *o124*, *o125* and *o126*, respectively.

According to the order in which the intruder performs operations in the process of calculating the availability zones of informative acoustic signals of the reconnaissance object, the average value $\overline{\omega}$ (*p13*) of the random value of the time spent by the intruder on the implementation of this mode of operation of the transmission control protocol (TCP), is determined according to the expression:

$$\overline{\omega}(p13) = \rho_{131}(\cdot o131\,\overline{\omega}) + \rho_{132}(\cdot o132\,\overline{\omega}) + \rho_{133}(\cdot o133\,\overline{\omega}) + \rho_{134}(\cdot o134\,\overline{\omega}) + \\ + E(\omega(o135)\,\omega^{\circ}(o136)\,\omega^{\circ}(o137)), \quad (3)$$

where ρ_{131}, ρ_{132}, ρ_{133} and ρ_{134} are the probabilities of performing operations *o131*, *o132*, *o133* and *o134* by the intruder in the process of illegal actions, respectively, $\overline{\omega}$ (*o131*), $\overline{\omega}$ (*o132*), $\overline{\omega}$ (*o133*) and $\overline{\omega}$ (*o134*) are the mean values of random values of time spent by the attacker to perform operations *o131*, *o132*, *o133*, and *o134*, respectively, and $E(\omega(o135)\circ(\omega(o136)\circ(\omega(o137))$ means the mean of the composition of the random variables $\omega(o135)$, $\omega(o136)$ and $\omega(o137)$ of the time the attacker performed operations *o135*, *o136* and *o137*, respectively.

The given order of operations performed by an intruder in the process of determining the places of optimal availability of informative acoustic signals of the reconnaissance object allows us to form an expression for the average value $\overline{\omega}$ (*p14*) of the random value of time spent by an intruder on the implementation of this mode of TCS operation, in the form:

$$\overline{\omega}(p14) = E(\omega(o141)\,\omega^{\circ}(o142)), \quad (4)$$

where $E(\omega(o141)\omega^{\circ}(o142))$ means the mean value of the composite of the random variables $\omega(o141)$ and $\omega(o142)$ of the time the attacker performed operations *o141* and *o142*, respectively.

In accordance with the given order of operations performed by an intruder in the process of interception of electrical signals modulated by informative acoustic signals with the help of AR conducting equipment through the channel of acousto-electrical transformations, the average value $\overline{\omega}$ (*p21*) of the random value of time spent by an intruder on the implementation of this mode of TCR operation, is determined in accordance with the expression:

$$\overline{\omega}\ (p21) = E(\omega\ (o211)\ \omega\ (o212)), \tag{5}$$

where $E(\omega\ (o211)\ \omega\ (o212))$ means the mean value of the composite of the random variables $\omega(o211)$ and $\omega\ (o212)$ of the time the attacker performed operations *o211* and *o212*, respectively.

The given order of operations performed by an intruder in the process of increasing the intelligibility of intercepted informative acoustic signals by special software (hardware-software) methods allows us to form an expression for the average value $\overline{\omega}$ (*p22*) of the random value of time spent by an intruder on the implementation of this mode of TCS operation, as follows:

$$\overline{\omega}\ (p22) = E(\omega\ (o221)\ \omega\ (o222)\ \omega\ (o223)), \tag{6}$$

where $E(\omega\ (o221)\ \omega\ (o222)\ \omega\ (o223))$ means the mean value of the composite of the random variables $\omega(o221), \omega\ (o222)$, and $\omega\ (o223)$ of the time the attacker performed operations *o221*, *o222*, and *o223*, respectively.

In accordance with the given order of operations performed by an intruder in the process of interception of over-repeated high-frequency (HF)-signals, modulated by informative acoustic signals in auxiliary technical means and systems (ATSS) of reconnaissance object by means of acoustic reconnaissance (AR) equipment via HF-irradiation channel, the average value $\overline{\omega}$ (*p31*) of random value of time, spent by an intruder on implementation of this mode of operation of ATSS, is determined according to the expression:

$$\overline{\omega}\ (p31) = E(\omega\ (o311)\ \omega\ (o312)), \tag{7}$$

where $E(\omega\ (o311)\ \omega\ (o312))$ means the mean value of the composite of the random variables $\omega(o311)$ and $\omega\ (o312)$ of the time the attacker performed operations *o311* and *o312*, respectively.

The given order of operations performed by an intruder in the process of increasing the intelligibility of intercepted informative acoustic signals by special hardware-software methods allows us to form an expression for the average value $\overline{\omega}$ (*p32*) of the random value of time spent by an intruder on the implementation of this mode of TCR operation, as follows:

$$\overline{\omega}\ (p32) = E(\omega\ (o321)\ \omega\ (o322)\ \omega\ (o323)), \tag{8}$$

where $E(\omega\ (o321)\ \omega\ (o322)\ \omega\ (o323))$ means the mean value of the composite of the random variables $\omega(o321), \omega\ (o322)$, and $\omega\ (o323)$ of the time the attacker performed operations *o321*, *o322*, and *o323*, respectively.

In accordance with the given order of operations performed by an intruder in the process of intercepting of re-transmitted HF signals, modulated by informative acoustic signals in VTSI of intelligence object by means of AR conducting equipment via HF-irradiation channel, the average value $\overline{\omega}$ (*p41*) of random value of time spent by an intruder on realization of this mode of TCR operation is determined according to the expression:

$$\overline{\omega}\ (p41) = E(\omega\ (o411)\ \omega\ (o412)\ \omega\ (o413)), \tag{9}$$

where $E(\omega\ (o411)\ \omega\ (o412)\ \omega\ (o413))$ means the mean value of the composite of the random variables $\omega(o411), \omega\ (o412)$, and $\omega\ (o413)$ of the time the attacker performed operations *o411*, *o412*, and *o413*, respectively.

The given order of operations performed by an intruder in the process of increasing the intelligibility of intercepted informative acoustic signals by special software (hardware-

software) methods allows us to form an expression for the average value $\overline{\omega}$ (*p42*) of the random value of time spent by an intruder on the implementation of this mode of TCR, in the form:

$$\overline{\omega}\,(p42) = E(\omega\,(o421)\ \omega\,(o422)\ \omega\,(o423)), \tag{10}$$

where $E(\omega\,(o421)\omega\,(o422)\omega\,(o423))$ means the mean value of the composite of the random variables $\omega(o421), \omega\,(o422)$, and $\omega\,(o423)$ of the time the attacker performed operations *o421*, *o422*, and *o423*, respectively.

According to the given order of operations performed by an intruder during interception of high-frequency electromagnetic signals arising during operation of generators included in the technical means and (or) parasitic (auto) generation in technical means of the intelligence object by means of AR conducting equipment via parasitic (auto) generation channel, the average value $\overline{\omega}$ (*p51*) of random value of time spent by an intruder on realization of this mode of TCR operation, is determined according to the expression:

$$\overline{\omega}\,(p51) = E(\omega\,(o511)\ \omega\,(o512)), \tag{11}$$

where $E(\omega\,(o511)\omega\,(o512))$ means the mean value of the composite of the random variables $\omega(o511)$ and $\omega\,(o512)$ of the time the attacker performed operations *o511* and *o512*, respectively.

The given order of operations performed by an intruder in the process of increasing the intelligibility of intercepted informative acoustic signals by special software (hardware-software) methods allows us to form an expression for the average value $\overline{\omega}$ (*p52*) of the random value of time spent by an intruder on the implementation of this mode of TCS operation, as follows:

$$\overline{\omega}\,(p52) = E(\omega\,(o521)\ \omega\,(o522)\ \omega\,(o523)), \tag{12}$$

where $E(\omega\,(o521)\omega\,(o522)\omega\,(o523))$ means the mean value of the composite of the random variables $\omega(o521), \omega\,(o522)$, and $\omega\,(o523)$ of the time the attacker performed operations *o521*, *o522*, and *o523*, respectively.

In accordance with the given order of operations performed by an intruder during the conversion of data intercepted through the channels of acousto-electrical transformations, RF irradiation, parasitic (auto) generation and RF imposition, the average value $\overline{\omega}$ (*p61*) of the random value of time spent by the intruder on the implementation of this mode of TCR operation, is determined according to the expression:

$$\overline{\omega}\,(p61) = E(\omega\,(o611)\ \omega\,(o612)), \tag{13}$$

where $E(\omega\,(o611)\omega\,(o612))$ means the mean value of the composite of the random variables $\omega(o611)$ and $\omega\,(o612)$ of the time the attacker performed operations *o611* and *o612*, respectively.

The given order of operations performed by an intruder during the search of information of interest allows us to form an expression to determine the average value $\overline{\omega}$ (*p62*) of the random value of time spent by an intruder on the implementation of this mode of TCR operation, in the form of:

$$\overline{\omega}\,(p62) = E(\omega\,(o621)\ \omega\,(o622)\ \omega\,(o623)), \tag{14}$$

where $E(\omega\,(o621)\omega\,(o622)\omega\,(o623))$ means the mean value of the composite of the random

variables $\omega(o621), \omega(o622)$, and $\omega(o623)$ of the time the attacker performed operations *o621*, *o622*, and *o623*, respectively.

In accordance with the given order of operations performed by an intruder during the analysis of sufficiency of information intercepted through the channels of acousto-electrical transformations, RF irradiation, parasitic (auto) generation and RF imposition for disclosure of information process content, the average value $\overline{\omega}(p63)$ of the random value of time spent by an intruder on implementation of this mode of TCR operation is determined according to the expression:

$$\overline{\omega}(p63) = E(\omega(o631)\ \omega^{\circ}(o632)), \tag{15}$$

where $E(\omega(o631)\omega^{\circ}(o632))$ means the mean value of the composite of the random variables $\omega(o631)$ and $\omega(o632)$ of the time the attacker performed operations *o631* and *o632*, respectively.

Time characteristics of intruder's capabilities to implement the stages of illegal actions to intercept information via parametric channels are formed on the third composite level of the system of characteristics of effectiveness of response measures to this kind of threats to information security. The formation procedure is based on the establishment of interlevel compositional links of these characteristics with the characteristics of the second level of this system.

3 Results and discussion

These studies are a continuation of the comprehensive experiment described in papers [1-4]. Assessment of the effectiveness of mechanisms for detecting threats to information leakage through parametric channels, in accordance with the above methodology, we will consider in relation to the typical characteristics of illegal actions to intercept information through the channels of the type under consideration and the typical characteristics of mechanisms for detecting threats to information leakage.

In order to implement this methodology, a set of programs to assess the effectiveness of mechanisms to identify threats to information leakage through parametric channels was developed. Figure 1 shows a dialog box to enter the initial data on the characteristics of threats in accordance with their representation in the form (22), obtained by analyzing the signs of illegal actions $_{ri}$, i = 1, 2, ..., 19 of their set) [5].

$$V = a \log 2A + b \log 2B \tag{16}$$

where: a - number of unique (non-repeating) actions performed to implement threats to information leakage through parametric channels (procedures for detecting such threats); A - total number of actions performed to implement such threats (procedures for detecting such threats); b - number of unique operands used to implement such actions (procedures); B - total number of operands used to implement threats to information leakage through parametric channels (procedures for detecting such threats).

The numerical characteristics of the calculations of the signs of illegal actions are shown in Figure 1.

№	IND	a	Amin	Amax	b	Bmin	Bmax	Vmin	Vmax	Vsr	Vsko
1	F1111	20	60	180	15	50	150	203	258	230	115
2	F1112	25	75	225	20	60	180	274	345	310	155
3	F1113	15	45	135	10	30	90	131	171	151	76
4	F1121	10	30	90	5	20	54	71	94	82	41
5	F1122	5	15	45	3	10	27	30	42	36	18
6	F1211	20	60	180	15	50	150	203	258	230	115
7	F1212	5	15	45	3	9	27	29	42	36	18
8	F1221	25	75	225	20	60	180	274	345	310	155
9	F1222	8	25	70	5	15	45	57	76	66	33
10	F2111	30	90	270	20	60	180	313	392	352	176
11	F2112	10	40	115	8	22	70	89	117	103	52
12	F2121	15	45	135	10	30	90	131	171	151	76
13	F2122	10	30	90	8	22	70	85	114	100	50
14	F2123	15	45	135	10	30	90	131	171	151	76
15	F2211	25	75	225	15	45	135	238	301	270	135
16	F2212	10	30	90	8	22	70	85	114	100	50
17	F2221	25	75	225	15	45	135	238	301	270	135
18	F2222	20	60	180	15	45	135	201	256	228	114

Fig. 1. Dialog box for entering initial data on the characteristics of information leakage threats through parametric channels.

In this case, the column "Identifier/IND" corresponds to the identifiers and names of the functions of the initial level of description of the threats of information leakage through parametric channels, the columns " α", "Amin", "Amax", " β", "Bmin", "Bmax" correspond to the parameters of expression (16).

The values in the columns "Vmin", "Vmax", "Vsr", "Vsko" correspond to the minimum, maximum, average values of the information volume of functions and its standard deviation, respectively. These values are determined in the process of the program complex operation.

On the basis of these initial data in accordance with the models presented in the paper, we obtain the values of information volume of functions of the third intermediate level of functional description of illegal actions to intercept information via parametric channels.

4 Conclusions

Obtained in the experiment, the values of the characteristics of the information volume of the target function of illegal actions to intercept the secondary HF radiation of the elements of radio-electronic equipment (REE) and semi-active pawning devices (SAPD) and the target function of detecting threats of information leakage through parametric channels can determine the effectiveness of mechanisms to detect threats to information leakage through parametric channels, that is, the effectiveness has increased to 78%:

$$E^{(в)} = 1 - \left(\frac{V}{V^{(y)}+V}\right) = 1 - (5152/(1496 + 5152))6 \approx 0{,}78. \quad (17)$$

Thus, the method of structuring the characteristics of mechanisms for detecting threats to information leakage through parametric channels presented in the work allows to provide significantly higher assessment reliability than the reliability of assessment by individual characteristics of mechanisms for detecting threats that are not connected in any system. The models considered in this paper are a methodological basis for synthesizing the procedure for assessing the effectiveness of mechanisms for detecting threats to information leakage via

parametric channels. The application of the evaluation of the effectiveness of mechanisms for detecting threats to information leakage through parametric channels developed in the article allows us to provide a more reliable assessment than traditional methods of assessment [6-10].

Thus, the article considers the optimal set of measures to respond to an attacker's operations of illegal interception of information via parametric channels when using the appropriate modes of operation of the TCP protocol, which reduces decision-making time, optimizes the system as a whole and significantly contributes to the optimization of its energy efficiency.

5 References

1. S.V. Belokurov, J.E. Lvovich, Noev A.N. et al., *Mathematical modeling of mechanisms for detecting threats of information leakage through parametric channels*, in Proceedings of the International Conference "Applied Mathematics, Computational Science and Mechanics: Current Problems", J. Phys.: Conf. Ser., **1202**. 012012 (2019)
2. S.V. Zapechnikov, N.G. Miloslavskaya, A.I. Tolstoy [et al] Information security of open systems: a textbook for universities. In 2 volumes. Volume 1. - Threats, vulnerabilities, attacks and approaches to protection. Moscow (2006)
3. Lamonov A.V. Safety of information technologies, **1** (2007)
4. V.A. Minaev, S.V. Skryl, S.V. Dvoryankin [et al] Informatika: textbook for higher educational institutions of the Ministry of Internal Affairs of Russia. Volume 1: Informatics: Conceptual Foundations. Moscow (2008)
5. Adam T. Elsworth, Electronic Warfare. Nova Science Publishers, Inc. (2011)
6. Anthimos Alexandros Tsirigotis, Cybernetics, Warfare and Discourse: The Cybernetisation of Warfare in Britain. Palgrave Macmillan (2017)
7. Darren Death, Information Security Handbook. Packt Publishing (2017)
8. Michael E. Whitman and Herbert J. Mattord, Principles of Information Security. Cengage Learning (2014)
9. Novikov D. New Frontiers in Information and Production Systems Modelling and Analysis: Incentive Mechanisms, Competence Management, Knowledge-based Production. Springer (2017)
10. Raymond Pompon. IT Security Risk Control Management. Apress (2016)
11. Richard A. Clarke, Robert Knake. Cyber War: The Next Threat to National Security and What to Do About It Paperback (2012)
12. Richard A. Poisel. Information Warfare and Electronic Warfare Systems. Artech House (2013)
13. John R. Vacca, Syngress. Network and System Security, Second Edition, 2nd Edition (2016)
14. William Stallings, Lawrie Brown. Computer Security: Principles and Practice, 3rd Edition. Pearson (2014)