Model of adaptive information security system of a computer-based data transmission network

L. M. Gruzdeva

Russian Transport University (MIIT)
9, bld. 9, Obrastsova str., Moscow, 127994, Russia

e-mail: docentglm@gmail.com

Abstract. The problem of increasing the capacity of a corporate data transmission network in the context of the impact of information security threats has been formalized as a task of constructing an adaptive information security system that is capable of providing the highest possible capacity level at a reliable detection of and maximum efficient counteraction to threats. A protection system model, which includes detection and counteraction levels whose facilities are promptly initiated in the most vulnerable nodes of the network, has been developed. In practice, this will shorten information threat detection time through elimination of traditional signal processing logics, as well as provide maximum possible counteraction to threats without a significant increase in the average packet delay time in the network.
Keywords: corporate data transmission network, information security system, information security, information threats.

1. Introduction

Despite measures taken to ensure information security (IS) of the resources of government agencies, large companies, small commercial organizations, etc., corporate data transmission networks (CDTN) still remain vulnerable to cyberattacks from external and internal intruders. Effective design, operation and upgrade of corporate networks in the context of the impact of information attacks are impossible without assessing performance quality indicators, with the network capacity being one of them [1–3].

The review of corporate network study activities and practical experience allows us to state a sharp decrease in the network capacity in the context of the impact of information attacks [4]. The decreased network capacity is associated with insufficient security due to the following reasons: broad use of open data transmission protocols; involvement of users of various categories in the data processing process and the use of dictionary passwords by these users; sensitive data storage in open/ public domains, etc. (Fig. 1, 2) [5].

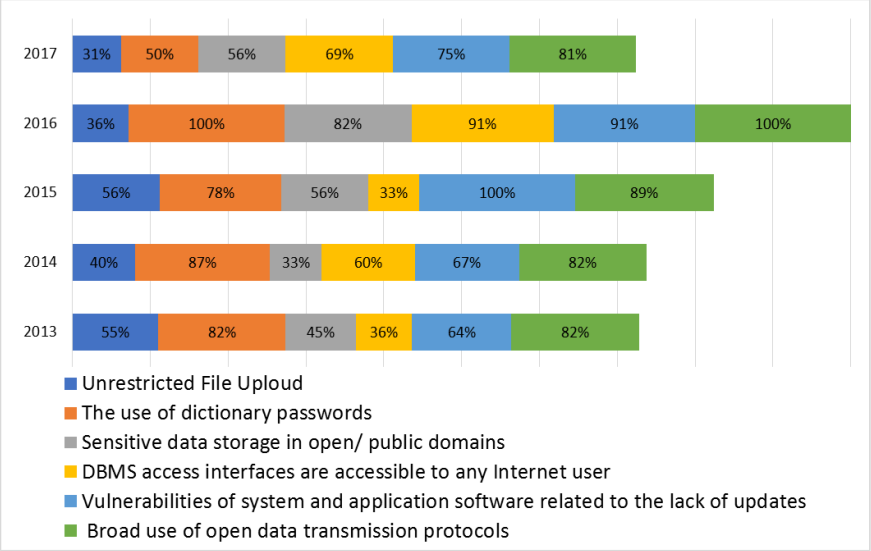

Figure 1. Most widespread the vulnerabilities on a network perimeter, discovered at the analysis of security (stake of the systems)

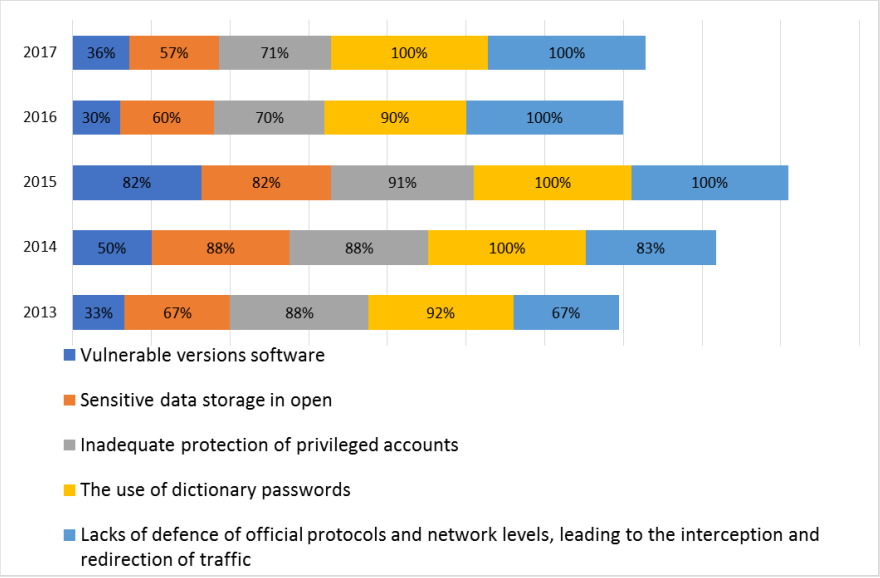

Figure 2. Most widespread the vulnerabilities, discovered at the analysis of security of intranet (stake of the systems)

The most common method, used by cybercriminals for cyberattacks, including those for gaining financial benefits, assumes the application of malicious software (MS), whose

share in 2017 reached 39% (Fig. 3) [6]. Criminals often combined this method with other methods, e. g., with social engineering or exploitation of web-vulnerabilities. In the first quarter of 2018, the share of MS-based attacks was 63% (+27% as compared to the similar period of 2017, Fig. 3) [7].

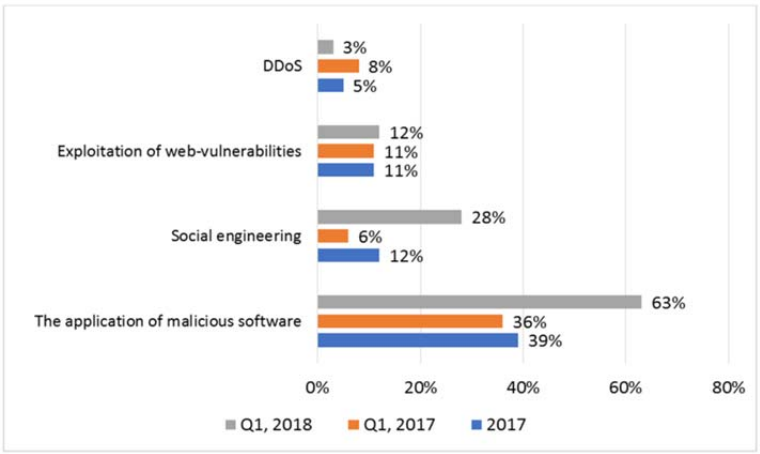

Figure 3. Methods, used by cybercriminals for cyberattacks

Advanced information security systems (ISS) [8, 9] solve this problem to some extent by partial blocking of harmful traffic; however, ensuring high detection probability and delays associated with counteractions, lead to a significant spending of network resources, which is ultimately accompanied by a decreased system capacity. Increasing the reliability of detection and identifying information attacks as well as developing methods and means to reduce their impact on the CDTN performance is so far and, obviously, will remain one of the urgent tasks for the nearest future.

2. Statement of the problem

Let there a set of corporate data transmission network objects $\{O_1, O_2, ..., O_K\}$ be given. Fig. 4 illustrates a structural scheme of the CDTN. Communication lines are absolutely reliable, noise-proof and consist of a duplex data channel; switching nodes (routers of CDTN segments) have an infinite memory; traffic consists of packets of the same priority and forms a Poisson stream; packet processing time at nodes is defined by the exponential distribution law.

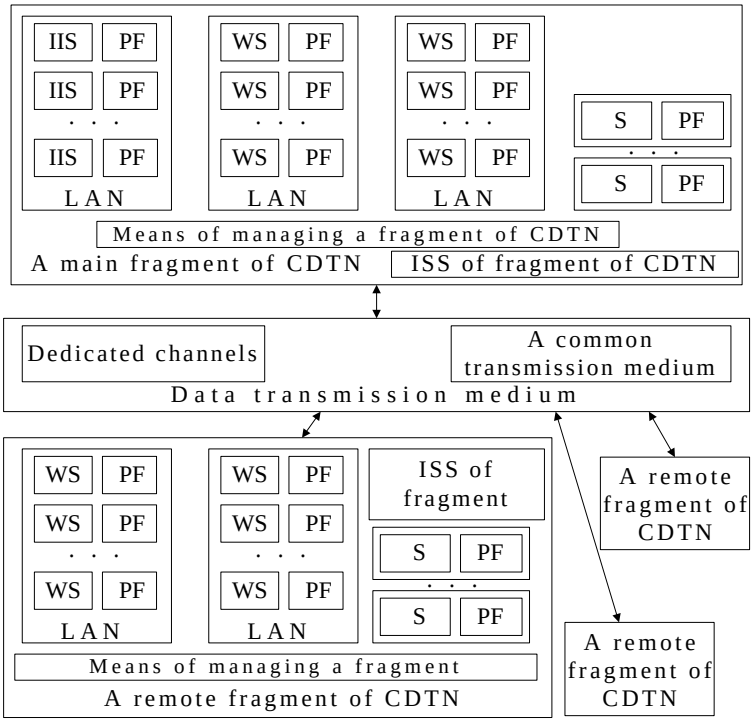

Figure 4. Structural scheme of the CDTN, where WS (workstation), PF (protection facilities), Local Area Network (LAN), Internet Information Services (IIS), Server (S)

It is required to ensure maximum possible CDTN capacity at a reliable detection and maximum effective counteraction to information security threats (information threats):

$$\begin{aligned} &\Phi(\Pi) \to \max; \\ &P_D(t) = \varphi_1(p_1(t),\ p_2(t), ...,\ p_N(t)) \to \max; \\ &\overline{P_{FA}}(t) = \varphi_2(\overline{p_1}(t),\ \overline{p_2}(t), ...,\ \overline{p_N}(t)) \to \max; \\ &Q_C(t) = \varphi_3(q_1(t),\ q_2(t), ...,\ q_K(t)) \to \max; \\ &T^D + T^C \le T^A. \end{aligned} \qquad (1)$$

where $\Phi(\Pi)$ — CDTN capacity; N — number of detection hardware $(N \ge K)$; $P_D(t)$ — probability of detecting IS threats; $\overline{P_{FA}}(t)$ — probability of a «false alarm» (FA) occurrence; K — number of countermeasures; $Q_C(t)$ — probability of counteraction to information threats; $T^D = \varphi_4(t_1^D, t_2^D, ..., t_N^D)$ — IS threat detection time; $T^D = \varphi_5(t_1^D, t_2^D, ..., t_K^D)$ — time for taking counteractions to IS threats; T^A — allowable time consumption for providing protection $(\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5)$ — types of corresponding functional dependencies).

The solution of the problem (1) involves the development of logic diagrams for reliable detection of information threats as well as the development of a distributed threat

counteraction system model. An adaptive information security system should be understood as a set of protection methods and facilities for a given number of corporate network objects, which requires minimum time for detecting an information attack at a simultaneous minimization of its consequences. The objective of the measures taken is to reduce the probability of a total infection of a corporate data network, mitigate consequences of such impacts and, thus, ensure the required CDTN capacity level.

3. Adaptive information security systems model

To solve this problem, an ISS was developed, whose functioning is convenient to be viewed on a structural model for detecting and countering information attacks to the CDTN resources (Fig. 5). Let's separate a high-level architecture of the information security system.

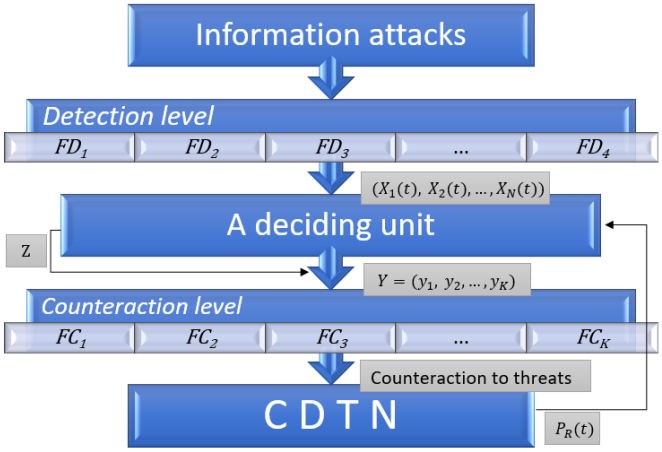

Figure 5. Structural model for detecting and countering information attacks to the CDTN resources

Detection level is a set of facilities of detecting information threats $FD = \{FD_1, FD_2, ..., FD_N\}$. Each element of the set FD has the following characteristics: $p_i(t), i = \overline{1,N}$ — probability of detecting information threats; $\bar{p}_i(t), i = \overline{1,N}$ — probability of "false alarm" occurrence; $t_i^D, i = \overline{1,N}$ — IS threat detection time that allows reaching maximum probability of detecting IS threats, i. e. $p_i^{\max} = \lim_{t \to t_i^D} p_i(t)$.

At the detecting hardware output, signal $X_i(t), i = \overline{1,N}$ is generated, which takes either 1 (information threat has been detected), or 0 (information threat has not been detect-

ed). Signal $X_i(t)$ by signal occurrence probability distribution densities — $f_y(X_i(t))$ (IS threat exists) and $f_n(X_i(t))$ (no IS threat):

$$f_y(X_i(t)) = \begin{cases} p_i(t) \text{ at } X_i(t) = 1, \\ 1 - p_i(t) \text{ at } X_i(t) = 1, \end{cases}$$

$$f_n(X_i(t)) = \begin{cases} p_i(t) \text{ at } X_i(t) = 1, \\ 1 - p_i(t) \text{ at } X_i(t) = 1. \end{cases}$$

While forming the detection level, the following conditions must be met:

1) ensure the possibility of combined operation of integrated detecting facilities;

2) ensure optimum operation time for detecting information security threats;

3) ensure given probability of information threat detection;

4) decrease the average frequency of "false alarms".

The study of detection level algorithms, which are based on traditional logic diagrams, has showed that easy signal processing and generation of a common decision on the presence or absence of information threats are the main advantage of these algorithms. A serious drawback of these algorithms is the ignorance of individual peculiarities and characteristics of each individual detecting facility, which does not allow achieving the best correlation between the probability of detection and frequency of generation of a "false alarm" at the detection level as a whole.

Paper [10] suggests a detection level operational logic that is based on the «critical area of threats» (CAT) notion. The advantage of this logic is the consideration of possible mutual influence of various detecting facilities, since CAT is configured based on probabilistic characteristics of the detection level, rather than its individual protection facilities.

A deciding unit implements the following logic: based on the detection level readings $(X_1(t), X_2(t), ..., X_N(t))$ a decision on the presence/ absence of information security threats is made:

$$Z = \begin{cases} 1 \text{ at information threat has been detected,} \\ 0 \text{ otherwise.} \end{cases}$$

If $Z = 1$, the control action $(y_1, y_2, ..., y_k)$, is generated, otherwise the algorithm ends.

Counteraction level is a combination of facilities for combatting information security threats $FC = \{FC_1, FC_1, ..., FC_K\}$, each of which can be initiated upon detection of a threat. Elements of the set FC have the following characteristics: $q_j(t)$, $j = \overline{1,K}$ — prob-

ability of countering information threats; t_j^C, $j = \overline{1,K}$ — counteraction time to reach maximum probability of countering IS threats, i. e. $q_j^{\max} = \lim_{t \to t_j^C} q_j(t)$.

Fig. 6 illustrates a schematic logic for initiating countermeasures to IS threats in an open corporate network.

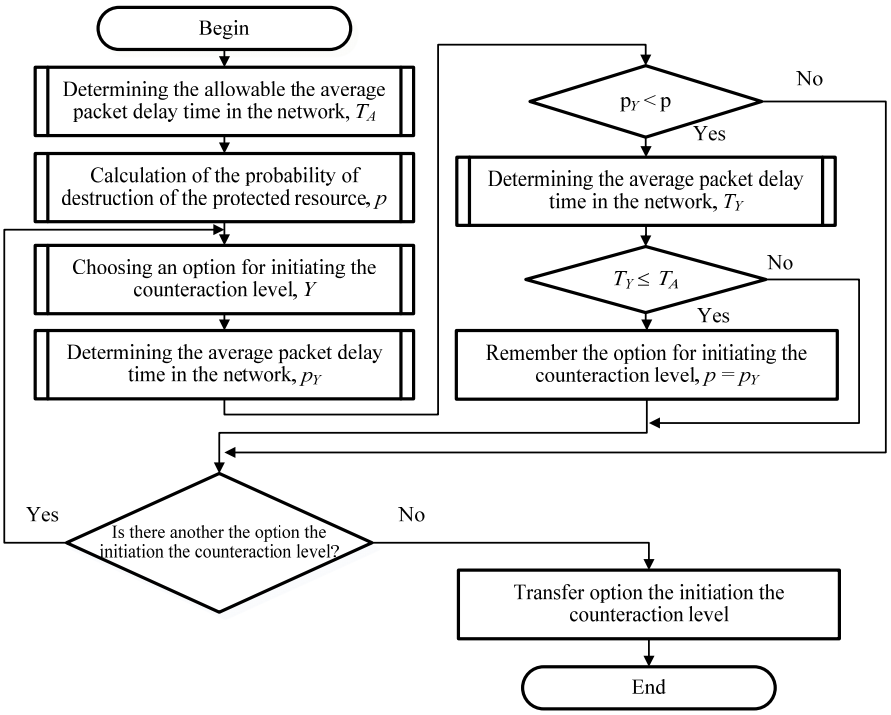

Figure 6. Schematic logic for initiating countermeasures in an open corporate network

Let's consider an open corporate network model comprising of a source of packets (node0) and a queueing system (QS) K $M/M/m_1/\infty, M/M/m_2/\infty, \ldots M/M/m_K/\infty$. Generally, an open queueing network (QN) is set by a stochastic routing matrix $P_R = \| p_{ij} \|$, where p_{ij} — is the probability of sending a packet from the $i-$th node to the $j-$th node, and $\sum_{j=0}^{K} p_{ij} = 1 \; \forall i = \overline{0,K}$. The average packet delay time in the network is one of its basic capacity parameters.

For context specificity, let's define the $K-$th node as a protected resource of an open queueing network. In each $i-$th node $(i = \overline{1,K-1})$, a counter facility that is capable with the probability u_i to counteract information security threats. This system includes

only $2^{(K-1)}-1$ counter facility initiation options, and the number thereof is numerically equal to the binary number:

$$Y=(y_1, y_2, ..., y_{K-1})_2$$

where $y_i=\begin{cases}0, \text{ if the countermeasure is not initiated at the } i\text{-th node,}\\ 1, \text{ if the countermeasure is initiated at the } i\text{-th node.}\end{cases}$

Let's imagine that a network runs a random process of spreading a malicious software, intended either for implementing IS threats to information processed in the network, or for a hidden misuse of resources or other impact that hampers normal operation of the network. In this case, the queueing network (QN) may be in one of discrete state $\{s_0, s_1, ..., s_K\}$. Transition from state s_i to state s_j occurs with the probability p_{ij} and means that malicious software of the $i-$th node has infected the $j-$th node $(i, j=\overline{0,K})$.

Suppose that the queueing network is initially in the state s_0, i. e. a malicious software is in the zero node (source of packets), whereas other nodes remain uninfected. As a result of a random a malicious software propagation process, susceptible nodes become infected.

The sequence of calculating the probability of counteraction to simple single non-return IS threats is as follows.

1. Plot matrix Q based on the elements of matrix P_R by introducing absorbing states s_0 and s_K into it (a malicious software may leave the system without infecting the K — th node).

$$Q=\begin{pmatrix}1 & 0 & 0 & ... & 0\\ p_{10} & p_{11} & p_{12} & \cdots & p_{1K}\\ p_{20} & p_{21} & p_{22} & ... & p_{2K}\\ ... & ... & ... & ... & ...\\ 0 & 0 & 0 & ... & 1\end{pmatrix}. \quad (2)$$

2. If there are no counter facilities in the system, then go to Step 3. Otherwise, based on the Y number, introduce an IS threat counter facility in (2). Let's consider that the counteraction means a malicious software outbreak to the 0-th node.

$$Q=\begin{pmatrix}1 & 0 & 0 & ... & 0\\ p_{10} & p_{11} & p_{12} & \cdots & p_{1K}\\ ... & ... & ... & ... & ...\\ p_{i0}+u_i(1-p_{i0}) & (1-u_i)p_{i1} & (1-u_i)p_{i2} & ... & (1-u_i)p_{iK}\\ ... & ... & ... & ... & ...\\ 0 & 0 & 0 & ... & 1\end{pmatrix},$$

where u_i $(i=\overline{1,K-1})$ — probability of a malicious software counteraction.

3. Set the probability distribution vector at the zero step:

$$e = (0,\ p_{01},\ p_{02}, ...,\ p_{01}).$$

4. Find the probability of distribution of the states at the n-th step using the formula: $q(n) = e \cdot Q^n$. Let's consider that a malicious software propagation process is completed at step n, if $p_1(n) = p_2(n) = ... = p_{K-1}(n) = 0$. The probability of the protected resource destruction is $p_Y = p_K(n)$, and the probability of counteraction is $Q_C(t) = p_0(n)$. The end of the sequence.

Simulation results. To implement this logic, an imitation simulation of a malicious software propagation process in a network with seven nodes was carried out. While processing data on all available options for initiating a counter facility $2^{(7-1)} - 1 = 63$, the following was revealed: in the existing network without a counter facility, the probability of infection is $p_0 = 0.550$; if a counter facility $(u = 0.9)$ is initiated in each node of the network, the probability is $p_{63} = 0.112$; and the average packet delay time T in the network has increased by ≈ 30%; if a counter facility is initiated only in the first, second and third nodes of the network, the probability is $p_{56} = 0.176$ and T has increased by ≈ 8%.

The sequence of calculating the probability of counteraction to simple single returnable IS threats is as follows.

1. Plot matrix Q based on the elements of matrix P_R by introducing absorbing states s_K into it (attack will continue until the K – th node is infected).

$$Q = \begin{pmatrix} 0 & p_{01} & p_{02} & \cdots & p_{0K} \\ p_{10} & p_{11} & p_{12} & \cdots & p_{1K} \\ p_{20} & p_{21} & p_{22} & \cdots & p_{2K} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}. \quad (3)$$

2. If there are no counter facilities in the system, then go to Step 3. Otherwise, based on the Y number, introduce an IS threat counter facility in (3). Let's consider that the counteraction means a malicious software outbreak to the (K + 1)-th node.

$$Q = \begin{pmatrix} 0 & p_{01} & \cdots & p_{0K} & 0 \\ p_{10} & p_{11} & \cdots & p_{1K} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (1-u_i)p_{i0} & (1-u_i)p_{i1} & \ldots & (1-u_i)p_{iK} & u_i \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & \ldots & 1 \end{pmatrix},$$

3. Set the probability distribution vector at the zero step:

$$e = (1,\ 0,\ 0,\ ...,\ 0).$$

4. Find the probability of distribution of the states at the $n-$th step using the formula: $q(n)=e\cdot Q^n$. Let's consider that a malicious software propagation process is completed at step n, if $p_1(n)=p_2(n)=...=p_{K-1}(n)=0$. The probability of the protected resource destruction is $p_K(n)$, and the probability of counteraction is $Q_C(t)=p_{K+1}(n)$. The end of the sequence.

Simulation results. The imitation simulation showed that the implementation of a threat to IS with a malicious software in an open queueing network without a counter facility will be successful at Step 45. If a counter facility is initiated only in the first node of the network, the highest probability of combatting IS treats is reached $Q_C(t)=p_8(22)=0.546$. (Table 1).

Table 1. Counteraction probabilities if a counter facility is initiated in one node of an open network

Counteraction probability	***Counter facility initiation option number***					
	$Y=32$	$Y=16$	$Y=8$	$Y=4$	$Y=2$	$Y=1$
	Random process completion pitch					
	$n=22$	$n=33$	$n=40$	$n=41$	$n=34$	$n=43$
$Q_C(t)$	0.546	0.405	0.498	0.408	0.435	0.398

The processing of the data on all countermeasure initiation options $2^{(7-1)}-1=63$ brought the following results: in the operating network, which does not include a counter facility, the probability of infection is $p_0=1.000$; if a counter facility $(u=0.7)$ is initiated in each node of the network, the probability is $p_{63}=0.145$ and the average packet delay time T in the network has increased by ≈ 30%; if a counter facility is initiated only in the first, second and third nodes of the network, the probability is $p_{60}=0.158$, and T has increased by ≈ 10%.

Implementation of the counteraction level initiation logic allows maximum possible counteraction to information security threats and required level of the system capacity.

4. Adaptive ISS operation logic

Launch detection level facilities. Detection time $t=0$.

Record signals from detecting facilities $X_1(t), X_2(t), ..., X_N(t)$.

If $X_1(t), X_2(t), ..., X_N(t)=0$ then information threats are not detected $(Z=0)$ and counteracting facilities are not launched. Go to step 2. Otherwise: $Z=1$.

Define probabilistic characteristics:

$P_D(t)=\varphi_1(p_1(t), p_2(t), ..., p_N(t))$ — probability of information threat detection by the detection level;

$\overline{P_{FA}}(t) = \varphi_2(\overline{p_1}(t), \overline{p_2}(t), ..., \overline{p_N}(t))$ — probability of «false alarm» (φ_1, φ_2 — types of corresponding functional dependencies);

$\Phi(P_D(t), \overline{P_{FA}}(t))$ — reliability criterion.

If the reliability criterion is below the threshold value $(\Phi(P_D(t), \overline{P_{FA}}(t)) \le \Phi_{th})$ information security threats have not been detected and counteraction level facilities are not launched. Go to Step 2. Otherwise: $Z = 1$.

Define a stochastic route matrix $P_R(t)$ [11].

Launch the logic for determining the CDTN nodes, which require the initiation of counteracting facilities. Control action is generated YyK $Y = (y_1, y_2, ..., y_K)$.

Initiate the counteraction level in accordance with the control action Y. The end of the algorithm.

5. Conclusion

The implementation of the suggested model of organizing protective mechanisms in a corporate data network provides the required capacity level by choosing an algorithm for early and reliable detection of information threats and by promptly initiating available facilities for countering information security threats in the most vulnerable nodes of the corporate network.

References

[1] *Olifer N., Olifer V.* (2006) *Computer Networks: Principles, Technologies and Protocols for Network Design. Hoboken*. NY, John Wiley & Sons, Inc.

[2] *Tanenbaum A. S., Wetherall D. J.* (2011) *Computer networks* (5th ed.), Pearson Hall.

[3] *Kurose J. F., Ross K. W.* (2013) *Computer networking: a top-down approach*. (6th ed.). Addison-Wesley.

[4] *Monakhov Yu. M., Gruzdeva L. M.* (2013) Teoreticheskoye i eksperimental'noye issledovaniye raspredelennykh telekommunikatsionnykh sistem v usloviyakh vozdeystviya vredonosnykh programm: monografiya. Vladimir, Izd-vo VlSU. [In Rus]

[5] *Corp. Vulnerabilities* (2018) https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Corporate-vulnerabilities-2018-rus.pdf [In Rus]

[6] *Cybersecurity threatscape* (2017) Retrieved from https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf [In Rus]

[7] *Cybersecurity threatscape* (2018) https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-Q1-rus.pdf [In Rus]

[8] *Jacobs S.* (2016) *Engineering information security: The application of systems engineering concepts to achieve information assurance* (2th ed.). John Wiley & Sons, Inc.

[9] *Vacca J.* (2017) *Computer and information security handbook* (3rd ed.) Morgan Kaufmann Inc.

[10] *Gruzdeva L. M., Monakhov M. Yu.* (2011) *Automation and Remote Control*, **72**(5):1075–1079. doi: 10.1134/S0005117911050158.

[11] *Vishnevsky V. M.* (2003) Teoreticheskiye osnovy proyektirovaniya komp'yuternykh setey. Moscow, Technosphere. [In Rus]

Модель адаптивной системы защиты информации компьютерной сети передачи данных

Л. М. Груздева

Российский университет транспорта (МИИТ), 127994, Москва, ул. Образцова, 9
e-mail: docentglm@gmail.com

Аннотация. Формализована задача повышения производительности корпоративной сети передачи данных в условиях воздействия угроз информационной безопасности, как задача построения адаптивной системы защиты информации, которая смогла бы обеспечить максимально возможный уровень производительности при достоверном обнаружении и максимально эффективном противодействии угрозам. Разработана модель системы защиты, включающая уровень обнаружения и уровень противодействия, средства которого оперативно инициируются в наиболее уязвимых узлах сети. Практическим результатом является сокращение времени обнаружения информационных угроз за счет отказа от традиционных алгоритмов логической обработки сигналов, а также максимально возможное противодействие без значительного увеличения средней задержки пакетов в сети.
Ключевые слова: корпоративная сеть передачи данных, система защиты информации, информационная безопасность, информационные угрозы.

Литература

[1] *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 5-е изд. — СПб. : Питер, 2016.

[2] *Tanenbaum A. S., Wetherall D. J.* Computer networks. — 5th ed. — Pearson Hall, 2011.

[3] *Kurose J. F., Ross K. W.* Computer networking: a top-down approach. 6th ed. by Pearson Education, Inc. publishing as Addison-Wesley, 2013.

[4] *Монахов Ю. М., Груздева Л. М.* Теоретическое и экспериментальное исследование распределенных телекоммуникационных систем в условиях воздействия вредоносных программ : монография. — Владимир : Изд-во ВлГУ, 2013.

[5] Positive Technologies. Уязвимости корпоративных информационных систем [Электронный документ] URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Corporate-vulnerabilities-2018-rus.pdf

[6] Positive Technologies. Актуальные киберугрозы — 2017: тренды и прогнозы [Электронный документ] URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf

[7] Positive Technologies. Актуальные киберугрозы I кв. 2018 года [Электронный документ] URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-Q1-rus.pdf

[8] *Jacobs S.* Engineering information security: The application of systems engineering concepts to achieve information assurance. — 2th ed. — John Wiley & Sons, Inc., 2016.

[9] *Vacca J.* Computer and information security handbook. — 3rd ed. — Morgan Kaufmann, 2017.

[10] *Gruzdeva L. M., Monakhov M. Yu.* Early detection algorithm for attacks against information resources of automatic manufacturing control systems // *Automation and Remote Control*. 2011. Vol. 72, No. 5. P. 1075–1079. doi: 10.1134/S0005117911050158.

[11] *Вишневский В. М.* Теоретические основы проектирования компьютерных сетей. — М. : Техносфера, 2003.

Автор:

Людмила Михайловна Груздева — кандидат технических наук, доцент кафедры «Информационно-математические технологии и информационное право», Российский университет транспорта (МИИТ)