DOI 10.31489/2019M4/127-135

UDC 94 (574): 340

B.K. Shayakhmetova[1], Sh.E. Omarova[2], V.G. Drozd[2]

[1] *Ye.A. Buketov Karaganda State University, Kazakhstan;*
[2] *Karaganda Economic University of Kazpotrebsoyuz, Kazakhstan*
(E-mail: kazahzavod@mail.ru)

Mathematical analysis of trend indicators of Internet security resources cyber-diagrams dynamics in the Republic of Kazakhstan

In the research the development of a mathematical model for predicting threats of information security of Internet resources is carried out, which allows, based on the minimum amount of input data, to indicate the dynamics of the development of possible threats in the life cycle of information systems, which may in the long run be a reason for shaping the costs of preventing threats to information security.

Keywords: mathematical model, predicting of threats, information security, life cycle, internet resource.

The global tendency characteristic of the last decades of introducing the achievements of information and communication technologies with a pace that is significantly ahead of the formation of a culture of their use, and the rooting of social and industrial relations characteristic of the «information society», primarily in matters of ensuring cybersecurity, also finds the confirmation.

New technologies, electronic services have become an integral part of our daily life. Given that, society is becoming increasingly dependent on information and communication technologies every day, the protection and availability of these technologies is becoming a critical moment and a very important topic for national interests.

Today, a necessary condition for the development of the information society is cybersecurity, which can be followed by a virtually endless list of security problems and their solutions, ranging from technical to legislative.

Traditionally, the concept of security is viewed through the prism of three approaches: the absence of threats, the security and stability of the system. It is obvious that the specific features of the development of the information space make the approach based on the understanding of security as the absence of threats irrelevant. In particular, in accordance with the interactive map of cyber threats of Kaspersky Lab, Kazakhstan is in the top 30 countries by the number of tested cyber attacks, most often taking place in the corridor between 18 and 27 places [1]. Thus, it makes sense to evaluate information security in contexts of relative security and the ability of the system to adequately respond to emerging challenges and threats, and minimize risks.

In world practice, as well as in the information segment of Kazakhstan, there is a steady trend of transferring information assets to Internet platforms and the provision of cloud services. The control of privileged users is one of the main tasks in relations with Internet service providers, software developers and technical support specialists. Now information assets of business and government structures can be placed anywhere, they are serviced by a large number of contractors scattered around the world, who, as a rule, are not responsible for violation of information security.

Thus, Internet service providers, while performing work in their segment of an information system, may accidentally or intentionally gain access to foreign systems, unauthorized launch applications or make configuration changes. Therefore, it is extremely difficult to limit their actions at the level of network access to applications by traditional means of delimiting and controlling access in information systems. In consequence of this, recently decisions on the control of Internet users will continue to be highly demanded in information systems, and this demand will increase every year.

In accordance with the international standard ISO / IE C 27001: 2005, information security incident management is an important element in ensuring the continuity of an organization's business processes [2]. Incident management is a process that is fed to the data received as a result of logging information about events related to information security, and the process output is informed about the reasons for the incident and measures that need to be taken to prevent the incident from happening again.

In general, incident management is a cyclical process, the main stages of which are represented by the PDCA model (Plan-Do-Check-Act, continuous improvement model of processes). According to ISO 27001,

the classical model includes four management stages: information security incident identification, information security incident response, investigation, corrective and preventive measures.

It is during the response and investigation of incidents that the specific information system vulnerabilities are revealed, traces of attacks and intrusions are detected, the operation of the protective equipment, the quality of the information security system architecture and its management are checked. Also important is the existence of procedures for analyzing and eliminating the consequences of incidents and taking corrective measures to reduce the likelihood of such incidents recurring in the future.

Thus, there is an urgent problem of prompt response to emerging incidents. It is necessary to decide which strategy out of the set of specific ones can be applied, or to determine that there is no suitable strategy and it is necessary to work it out (Table 1).

Table 1

The number of cyber incidents registered in Kazakhstan that violate the information security of users of Internet resources for the period from 2015–2017

№	Incident Type	Quantity in 2015	Quantity in 2016	Quantity in 2017	Total
1	Unauthorized access and modification of the content of Internet resources (website defacement) / attacks on an Internet resource	588	1934	658	3180

Note. Source: State Technical Service https://lsm.kz/kakie-banki-podvergalis-kiberatakam-v-2017-godu.

One of the promising areas of research for solving the problem of protection against cyber attacks on IP is the creation of methods for predicting their intensity by means of mathematical methods of analysis [3–13]. Note that the intensity of cyber attacks is the total number of these attacks per unit of time. In the case of a forecast that the intensity of cyber attacks on IP exceeds a certain predetermined value, additional measures of protection can be taken, including, for example, a more in-depth intelligent analysis of traffic [14–20].

In recent years, an increasing interest of researchers in trend analysis and prediction of cyber attacks has been observed [21–24]. This can be explained by the fact that trend forecasts make it possible to receive not only forecasts of directly future events, but also characterizing their estimates.

An important method of stochastic predictions is the exponential smoothing method. This method consists in the fact that a number of dynamics is smoothed with the help of a moving average in which the weights obey the exponential law [25, 26].

A special feature of the exponential smoothing method is that the procedure for finding the smoothed level uses only the previous levels of the series, taken with a certain weight, and the weight decreases as it moves away from the point in time for which the smoothed value of the series level is determined. If for the initial time series y_1, y_2, y_3,..., y_n the corresponding smoothed values of the levels are denoted by S_t, $t = 1,2,...,n$, this exponential smoothing is carried out according to the formula: $S_t = (1-\alpha)yt + \alpha S_{t-1}$.

Some sources give a different formula: $S_t = \alpha yt+(1-\alpha)S_{t-1}$, where α — smoothing parameter ($0 < \alpha < 1$); magnitude (1-α) called the discount factor.

In practical tasks of processing economic time series, it is recommended (unreasonable) to choose the value of the smoothing parameter in the range from 0,1 to 0,3. There are no other precise recommendations for choosing the optimal value of the parameter α. In some cases, it is proposed to determine the value of α based on the length of the series being smoothed: $\alpha = 2/(n+1)$.

As for the initial parameter S_0, then in tasks it is taken or equal to the value of the first level of the series Гі$_1$, or equal to the arithmetic average of the first few terms of the series. If, at the approach to the right end of the time series, the values smoothed by this method with the selected parameter α begin to differ significantly from the corresponding values of the original series, it is necessary to switch to another smoothing parameter. The advantage of this method is that with smoothing, neither the initial nor the final levels of the smoothing time series are lost. As S_0 take the first value of the row, $S_0 = y_1 = 588$ (Table 2).

Table 2

Calculated parameters of the model equation

t	y	S_t	Formula	$(y - S_t)^2$
2015	588	588	(1 – 0,3)*588 + 0,3*588	0
2016	1934	1530,2	(1 – 0,3)*1934 + 0,3*588	163054,44
2017	658	919,66	(1 – 0,3)*658 + 0,3*1530,2	68465,956
				231520,396

Note. The table is based on the calculation.

Forecasting data using exponential smoothing:

The prediction methods called «smoothing» take into account the effects of the overshoot function much better than the methods using regression analysis.

The basic equation is as follows:

S(t+1) = S(t)(1 - α) + αY(t)

S(t) – this is a forecast made at a time t;

S(t+1) reflects the forecast in the time period immediately following the point in time t :

$S(3+1) = 919,66(1 - -0,3) + 0,3 * 658 = 841,162.$

Standard error (error) is calculated by the formula:

$$e_t = \sqrt{\frac{\sum (y_i - S_{i-1})^2}{n-1}},$$

where i = (t - 2, t)

$$e_t = \sqrt{\frac{231520,396}{3-1}} = 340,236.$$

The linear trend equation has the form: $y = bt + a$.

1. Find the parameters of the equation by the method of least squares:

The OLS system of equations takes the form:

$an + b\sum t = \sum y$

$a\sum t + b\sum t^2 = \sum y*t$ (Table 3).

Table 3

Calculated parameters in tabular form

t	y	t^2	y^2	t y
1	588	1	345744	588
2	1934	4	3740356	3868
3	658	9	432964	1974
6	3180	14	4519064	6430
Average value	1060	4.667	1506354.667	2143.333

Note. The table is based on the calculation.

For our data, the system of equations is:

$3\ a + 6\ b = 3180$

$6\ a + 14\ b = 6430.$

From the first equation we express a and substitute in the second equation.

Get $a = 990$, $b = 35$.

Get the trend equation: $y = 35\ t + 990$.

Empirical trend coefficients a and b are only estimates of theoretical coefficients β_i, and the equation itself reflects only a general tendency in the behavior of the variables in question.

Trend ratio $b = 35$ shows the average change in the effective index (in units of y) with a change in the time period t per unit of measurement. In this example, with t by 1 unit, y change on average by 35.

Estimate the quality of the trend equation using the average relative approximation error.

$$\overline{A} = \frac{\sum |y_t - y_i| : y_i}{n} 100\ \%.$$

The approximation error within 5 %–7 % indicates a good selection of the trend equation to the source data.

$$\overline{A} = \frac{1,8592}{3} 100\% = 61,97\ \%.$$

To determine the size of the error or accuracy of the forecast indicator Y calculate the coefficient of disparity Teil formula:

$$K_T = \frac{\sqrt{\sum (y_i - \overline{y})^2}}{\sqrt{\sum y_t^2}};$$

$$K_T = \frac{1145814}{4519064} = 0,254.$$

This indicator varies from 0 to 1. The closer its value is to zero, the better the prediction results.

Average values:

$$\overline{t} = \frac{\sum t_i}{n} = \frac{6}{3} = 2;$$

$$\overline{y} = \frac{\sum y_i}{n} = \frac{3180}{3} = 1060;$$

$$\overline{t \cdot y} = \frac{\sum t_i y_i}{n} = \frac{6430}{3} = 2143,3333.$$

Dispersion:

$$D(t) = \frac{\sum t_i^2}{n} - \overline{t}^2 = \frac{14}{3} - 2^2 = 0,6667;$$

$$D(y) = \frac{\sum y_i^2}{n} - \overline{y}^2 = \frac{4519064}{3} - 1060^2 = 382754,6667.$$

Standard deviation:

$$\sigma(t) = \sqrt{D(t)} = \sqrt{0,6667} = 0,8165;$$

$$\sigma(y) = \sqrt{D(y)} = \sqrt{382754,6667} = 618,6717.$$

Calculate the coefficient of determination:

$$R^2 = 1 - \frac{\sum (y_i - y_t)^2}{\sum (y_i - \overline{y})^2};$$

$$R^2 = 1 - \frac{1145814}{1148264} = 0,00213,$$

where in 0,21 % of cases, t affects the change y. In other words — the accuracy of the selection of the trend equation is low.

To assess the quality of the parameters of the equation, we construct a calculation table (Table 4).

Table 4

Calculated parameters in tabular form

t	y	y(t)	$(y_i\text{-}y_{cp})^2$	$(y_i\text{-}y(t))^2$	$(y_i\text{-}y(t)) : y_i$
1	588	1025	222784	190969	0,743
2	1934	1060	763876	763876	0,452
3	658	1095	161604	190969	0,664
		3180	1148264	1145814	1,859

Note. The table is based on the calculation.

2. Analysis of the accuracy of determining estimates of the parameters of the trend equation:
Dispersion error equation:

$$S_y^2 = \frac{\sum (y_i - y_t)^2}{n - m - 1},$$

where m = 1 — the number of influencing factors in the trend model.

$$S_y^2 = \frac{1145814}{1} = 1145814.$$

Standard equation error:

$$S_y = \sqrt{S_y^2} = \sqrt{1145814} = 1070,427;$$

$$S_b = S_y \cdot \frac{\sqrt{\sum t^2}}{n\sigma_t};$$

$$S_b = 1070,427 \cdot \frac{\sqrt{14}}{3 \cdot 0,8165} = 1635,104;$$

$$S_a = \frac{S_y}{\sqrt{n}\sigma_t} = \frac{1070,427}{0,8165\sqrt{3}} = 756,906.$$

Perform interval forecast and determine the standard error of the predicted indicator.
$Uy = y_{n+L} \pm K$,
where

$$K = t_a \cdot S_y \cdot \sqrt{1 + \frac{1}{n} + \frac{3(n + 2L - 1)^2}{n(n^2 - 1)}},$$

L — lead period; y_{n+L} — point forecast by model on $(n + L)$ moment of time; n — number of observations in the time series; Sy — standard prediction error; T_{tabl} — the tabular value of student's criterion for the level of significance α and for the number of degrees of freedom equal to *n-2*.
According to the student's table we find T_{tabl}
T_{tabl} (*n-m-1*;$\alpha/2$) = (;) = 12,706.
Spot forecast, t = 4: y(4) = 35*4 + 990 = 1130.

$$K_1 = 12,706 \cdot 1070,43 \cdot \sqrt{1 + \frac{1}{3} + \frac{3\,(3 + 2 \cdot 1 - 1)^2}{3\,(3^2 - 1)}} = 24831,63.$$

1130 – 24831,63 = -23701,63; 1130 + 24831,63 = 25961,63.
Interval forecast:
t = 4: (-23701,63;25961,63)
Spot forecast, t = 5: y(5)= 35*5 + 990 = 1165.

$$K_2 = 12,706 \cdot 1070,43 \cdot \sqrt{1 + \frac{1}{3} + \frac{3\,(3 + 2 \cdot 2 - 1)^2}{3\,(3^2 - 1)}} = 32849,16.$$

1165 – 32849,16 = -31684,16; 1165 + 32849,16 = 34014,16.
Interval forecast:
t = 5: (-31684,16;34014,16).
Spot forecast, t = 6: y(6)= 35*6 + 990 = 1200.

$$K_3 = 12,706 \cdot 1070,43 \cdot \sqrt{1 + \frac{1}{3} + \frac{3\,(3 + 2 \cdot 3 - 1)^2}{3\,(3^2 - 1)}} = 41551,27.$$

1200 - 41551.27 = -40351,27; 1200 + 41551,27 = 42751,27.

Interval forecast:
t = 6: (-40351,27;42751,27)
Spot forecast, t = 7: y(7) = 35*7 + 990 = 1235.

$$K_4 = 12,706 \cdot 1070,43 \cdot \sqrt{1 + \frac{1}{3} + \frac{3\left(3 + 2 \cdot 4 - 1\right)^2}{3\left(3^2 - 1\right)}} = 50585,88.$$

1235 – 50585,88 = -49350,88; 1235 + 50585,88 = 51820,88.
Interval forecast:
t = 7: (-49350,88;51820,88)
3. Testing hypotheses regarding the coefficients of the linear trend equation:
1) t- statistics. Student criterion.
According to the student's table we find T_{tabl}
T_{tabl} (n-m-1;$\alpha/2$) = (1;0,025) = 12,706.

$$t_a = \frac{a}{S_a};$$

$$t_a = \frac{35}{756,906} = 0,04624 < 12,706.$$

The statistical significance of the coefficient a is not confirmed

$$t_b = \frac{b}{S_b};$$

$$t_b = \frac{99035}{1635,104} = 0,6055 < 12,706.$$

2) F- statistics. Fisher Criterion.
Coefficient of determination:

$$F = \frac{R^2}{1 - R^2} \frac{n - m - 1}{m} = \frac{0,00213}{1 - 0,00213} \frac{3 - 1 - 1}{1} = 0,00214.$$

Find from the table Fkp(1;1;0.05) = 161,
where m — the number of factors in the trend equation (m=1).

Insofar as $F < Fkp$, then the coefficient of determination (and, in general, the trend equation) is not statistically significant.

As a result of the study, the time dependence was studied Y from time t. At the specification stage, a linear trend was chosen. Its parameters are estimated by the method of least squares. The statistical significance of the equation is verified using the coefficient of determination and the Fisher criterion. It was found that in the situation under study, 0.21 % of the total variability Y due to the change in the time parameter. It was also established that the parameters of the model are not statistically significant. Economic interpretation of model parameters is possible — with each time period t value Y on average, increases by 35 units.

Thus, when creating an IP protection system to counter cyber attacks, in addition to implementing the information risk management system, their information audit and analysis, it is necessary to pay attention to predicting the intensity of cyber attacks.

As follows from the results of this work, interval forecasting of the intensity of cyber attacks on informatization objects of critical infrastructures is an important practical task. Experimental studies of interval prediction of cyber attack intensity by means of trend extrapolation methods with dynamic updating of the smoothing parameter showed that the proposed approach has the best accuracy of interval prediction of a selected indicator of cyber attack intensity.

References

1 Сайт компании «Лаборатория Касперского» [Электронный ресурс]. – Режим доступа: https://cybermap.kaspersky.com/ru/.

2 Сайт «Международная организация по стандартизации» [Электронный ресурс]. – Режим доступа: https://www.iso.org/standard/42103.html

3 Петренко С.А. Концепция раннего распознавания и предупреждения компьютерного нападения / С.А. Петренко, А.С. Петренко // Информационные системы и технологии в моделировании и управлении: материалы Всеросс. науч.-практ. конф. — 2016. – С. 82–86.

4 Петренко С.А. Национальная система раннего предупреждения о компьютерном нападении / С.А. Петренко, Д.Д. Ступин. – Иннополис: Изд. дом «Афина», 2017. – 440 с.

5 Werner G. Time series forecasting of cyber-attack intensity / G. Werner, S. Yang, K. McConky // Proceedings of the 12th Annual Conference on Cyber and Information Security. – 2017. – P. 224–240.

6 Гамбаров Г.М. Статистическое моделирование и прогнозирование: учеб. пос. / Г.М. Гамбаров, Н.М. Журавель, Ю.Г. Королев и др.; под ред. А.Г. Гранберга. – М.: Финансы и статистика, 1990. – 383 с.

7 Малюк А.А. Защита информации: современные проблемы / А.А. Малюк // Безопасность информационных технологий. — 2010. — № 1. — С. 5–9.

8 Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. — Киев: Изд-во «Диасофт», 2004. — 992 с.

9 Малюк А.А. К вопросу об интенсификации процессов защиты информации / А.А. Малюк // Безопасность информационных технологий. — 2011. — № 1. — С. 6–10.

10 Малюк А.А. Информационная безопасность; концептуальные и методологические основы защиты информации: учеб. пос. для вузов / А.А. Малюк. — М.: Горячая линия-Телеком, 2004. — 280 с.

11 Герасименко В.А. Основы защиты информации / В.А. Герасименко, А.А. Малюк. — М.: МИФИ, 1997. — 537 с.

12 Ажмухамедов И.М. Принципы обеспечения комплексной безопасности информационных систем / И.М. Ажмухамедов // Вестн. АГТУ. Сер. Управление, вычислительная техника и информатика. — 2011. — № 1. — С. 7–11.

13 Скородумов Б.И. О понятийно-терминологическом аппарате информационной безопасности / Б.И. Скородумов // БИТ. — 2008. — № 4. — С. 43–45.

14 Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пос. / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. — 416 с.

15 Партыка Т.Л. Информационная безопасность: учеб. пос. / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2012. — 432 с.

16 Борисов В.В. Компьютерная поддержка сложных организационно-технических систем / В.В. Борисов, И.А. Бычков, А.В. Дементьев, А.П. Соловьев, А.С. Федулов. – М.: Горячая линия – Телеком, 2002. – 154 с.

17 Ажмухамедов И.М. Математическая модель комплексной безопасности компьютерных систем и сетей на основе экспертных суждений / И.М. Ажмухамедов // Инфокоммуникационные технологии. — 2009. — 7. — № 4. — С. 103–107.

18 Войтик А.И. Экономика информационной безопасности: учеб. пос. / А.И. Войтик, В.Г. Прожерин. – СПб.: НИУИТМО, 2012. – 120 с.

19 Вестник УрФО. Безопасность в информационной сфере [Электронный ресурс]. — Режим доступа:http://www.info-secur.ru/

20 Ажмухамедов И.М. Моделирование на основе экспертных суждений процесса оценки информационной безопасности / И.М. Ажмухамедов // Вестн. АГТУ. Сер. Управление, вычислительная техника и информатика. — 2009. — 2. — С. 101–109.

21 Ларина И.Е. Экономика защиты информации: учеб. пос. / И.Е. Ларина. — М.: МГИУ, 2007. — 92 с.

22 Ажмухамедов И.М. Повышение безопасности компьютерных систем и сетей на основе анализа сетевого трафика / И.М.Ажмухамедов, А.Н. Марьенков // Инфокоммуникационные технологии. — 2010. — 8. — № 3. — С. 106–108.

23 Сайт компании «Лаборатория Касперского» [Электронный ресурс]. — Режим доступа: http://media.kaspersky.com/.

24 Aamodt A. Case-Based Reasoning: Foundational Issues, methodological Variations, and System Approaches / A. Aamodt, E. Plaza // AI Communications. — 1994. — 7. — No. 1. — P. 39–59.

25 Люгер Д.Ф. Искусственный интеллект: стратегии и методы решения сложных проблем / Д.Ф. Люгер. — М.: Вильямс, 2003. — 864 с.

26 Берман А.Ф. Концепция построения прецедентной экспертной системы / А.Ф. Берман, О.А. Николайчук, А.И. Павлов, А.Ю. Юрин // Междунар. конф. по вычислительной механике и современным прикладным программным системам. — 2003. — 2. — С. 110, 111.

Б.К. Шаяхметова, Ш.Е. Омарова, В.Г. Дрозд

Қазақстан Республикасындағы интернет-қауіпсіздік ресурстарының кибер-диаграммалары динамикасының үрдістік көрсеткіштерін математикалық талдау

Мақалада интернет-ресурстардың ақпараттық қауіпсіздігіне қауіп-қатерлерді алдын ала болжау үшін математикалық модель әзірленген, бұл енгізілген деректердің ең аз мөлшеріне сүйене отырып, ақпараттық жүйелердің өмірлік циклінде мүмкін қауіптердің даму динамикасын көрсетуге мүмкіндік береді, бұл болашақта ақпарат қауіпсіздігіне төнетін қатердің алдын-алуға, шығындардың қалыптасуына әкелуі мүмкін.

Кілт сөздер: математикалық модель, қауіптерді болжау, ақпараттық қауіпсіздік, өмірлік цикл, интернет-ресурстар.

Б.К. Шаяхметова, Ш.Е. Омарова, В.Г. Дрозд

Математический анализ трендовых показателей динамики кибер-диаграмм ресурсов интернет-безопасности в Республике Казахстан

В статье разработана математическая модель прогнозирования угроз информационной безопасности интернет-ресурсов, позволяющая на основе минимального объема исходных данных указать динамику развития возможных угроз в жизненном цикле информационных систем, что может явиться в перспективе основанием по формированию затрат на предотвращение угроз информационной безопасности.

Ключевые слова: математическая модель, прогнозирование угроз, информационная безопасность, жизненный цикл, интернет-ресурсы.

References

1 Sait kompanii «Laboratoriia Kasperskoho» [The site of the company «Kaspersky laboratory»]. *kaspersky.com.* Retrieved from https://cybermap.kaspersky.com/ru/ [in Russian].

2 Sait «Mezhdunarodnaia orhanizatsiia po standartizatsii» [Sait of «ISO»]. *iso.org.* Retrieved from https://www.iso.org/standard/42103.html.

3 Petrenko, S.A., & Petrenko, A.S. (2016). Kontseptsiia ranneho raspoznavaniia i preduprezhdeniia kompiuternoho napadeniia [The concept of early detection and prevention computer attacks]. *Materialy Vserossiiskoi nauchno-prakticheskoi konferentsii «Informatsionnye sistemy i tekhnolohii v modelirovanii i upravlenii»,* 82–86 [in Russian].

4 Petrenko, S.A., & Stupin, D.D. (2017). *Natsionalnaia sistema ranneho preduprezhdeniia o kompiuternom napadenii [National Computer Attack Early Warning System].* Innopolis: Izdatelskii Dom «Afina» [in Russian].

5 Werner, G. Yang, S., & McConky, K. (2017). Time analysis of cyber-attack intensity *Proceedings of the 12th Annual Conference on Cyber and Information Security*, 224–240.

6 Gambarov, G.M., Zhuravel, N.M., & Korolev, Yu.G., et. al. (1990) *Statisticheskoe modelirovanie i prohnozirovanie [Statistical modeling and forecasting].* Moscow: Finansy i statistika [in Russian].

7 Maliuk, A.A. (2010). Zashchita informatsii: sovremennye problemy [Information security: current problems]. *Bezopasnost informatsionnykh tekhnolohii, 1,* 5–9 [in Russian].

8 Domarev, V.V. (2004). *Bezopasnost informatsionnykh tekhnolohii. Sistemnyi podkhod [Security information technology. System approach].* Kiev: Izdtelstvo «Diasoft» [in Russian].

9 Maliuk, A.A. (2011). K voprosu ob intensifikatsii protsessov zashchity informatsii [To the question of the intensification of information security processes]. *Bezopasnost informatsionnykh tekhnolohii, 1*, 6–10 [in Russian].

10 Maliuk, A.A. (2004). *Informatsionnaia bezopasnost: kontseptualnye i metodolohicheskie osnovy zashchity informatsii [Information Security: conceptual and methodological foundations of information security].* Moscow: Hotline-Telecom [in Russian].

11 Gerasimenko, V.A., & Malyuk, A.A. (1997). *Osnovy zashchity informatsii [Basics of information security].* Moscow: MEPI [in Russian].

12 Azhmukhamedov, I.M. (2011). Printsipy obespecheniia kompleksnoi bezopasnosti informatsionnykh sistem [Principles of ensuring integrated security of information systems]. *Bulletin of ASTU. Series Management, Computer Engineering and Informatics, 1*, 7-11 [in Russian].

13 Skorodumov, B.I (2008). O poniatiino-terminolohicheskom apparate informatsionnoi bezopasnosti [On the conceptual and terminological apparatus of information security]. *BIT, 4*, 43-45 [in Russian].

14 Shangin, V.F. (2013). *Informatsionnaia bezopasnost kompiuternykh sistem i setei [Information security of computer systems and networks].* Moscow: ID FORUM; SIC INFRA-M [in Russian].

15 Partyka, T.L., & Popov, I.I. (2012). *Informatsionnaia bezopasnost [Information Security].* Moscow: Forum [in Russian].

16 Borisov, V.V., Bychkov, I.A., Dementev, A.V., Solovev, A.P., & Fedulov, A.S. (2002). *Kompiuternaia podderzhka slozhnykh orhanizatsionno-tekhnicheskikh sistem [Computer support for complex organizational and technical systems].* Moscow: Hotline - Telecom [in Russian].

17 Azhmukhamedov, I.M. (2009). Matematicheskaia model kompleksnoi bezopasnosti kompiuternykh sistem i setei na osnove ekspertnykh suzhdenii [Mathematical model of integrated security of computer systems and networks based on expert judgments]. *Infocommunication technologies Vol. 7, 4,* 103–107 [in Russian].

18 Voitik, A.I. (2012). *Ekonomika informatsionnoi bezopasnosti [The Economics of Information Security].* Saint Petersburg: NIUITMO [in Russian].

19 Sait zhurnala «Vestnik UrFO. Bezopasnost v informatsionnoi sfere» [Site of Journal «Bulletin of the Ural Federal District. Information Security information security»]. *info-secur.ru.* Retrieved from http://www.info-secur.ru/ [in Russian].

20 Azhmukhamedov, I.M. (2009). Modelirovanie na osnove ekspertnykh suzhdenii protsessa otsenki informatsionnoi bezopasnosti [Modeling on the basis of expert judgments of the information security assessment process]. *ASTU Bulletin. Series: Management, Computer Engineering and Informatics, 2*, 101–109 [in Russian].

21 Larina, I.Ye. (2007). *Ekonomika zashchity informatsii [The Economics of Information Security].* Moscow: MHIU [in Russian].

22 Azhmukhamedov, I.M., & Marienkov, A.N. (2010). Povyshenie bezopasnosti kompiuternykh sistem i setei na osnove analiza setevoho trafika [Improving the security of computer systems and networks based on network traffic analysis]. *Infocommunication Technologies, Vol. 8, 3,* 106–108 [in Russian].

23 Sait kompanii «Laboratoriia Kasperskoho» [The sait of company «Kaspersky Lab»]. *kaspersky.com.* Retrieved from http://media.kaspersky.com/ [in Russian].

24 Aamodt, A., & Plaza, E. (1994). Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches. *AI Communications, Vol. 7, 1,* 39–59.

25 Luger D.F. (2002). *Iskusstvennyi intellekt: stratehii i metody resheniia slozhnykh problem [Artificial Intelligence: Strategies and Methods for Solving Difficult Problems].* Moscow: Williams [in Russian].

26 Berman, A.F., Nikolaichuk, O.A., Pavlov, A.I., & Yurin, A.Yu. (2003). Kontseptsiia postroeniia pretsedentnoi ekspertnoi sistemy [The concept of building a precedent expert system]. *International Conference on Computational Mechanics and Modern Applied Software Systems, 2,* 110–111 [in Russian].