Models of forecasting destructive influence risks for information processes in management systems

V. G. Anisimov[a], *Dr. Sc., Tech., Professor, orcid.org/ 0000-0002-5097-4618, an-33@yandex.ru*
E. G. Anisimov[b], *Dr. Sc., Tech., Professor orcid.org/ 0000-0002-6527-2352*
T. N. Saurenko[b], *Dr. Sc., Econ., Head of Chair, orcid.org/ 0000-0003-1736-7178*
E. A. Zotova[a], *Assistant Professor, orcid.org/ 0000-0003-4539-4253*
[a]*Peter the Great St. Petersburg Polytechnic University, 29, Politekhnicheskaia St., 195251, Saint-Petersburg, Russian Federation*
[b]*Peoples' Friendship University of Russia (RUDN University), 6, Miklukho-Maklay St., 117198, Moscow, Russian Federation*

Introduction: *One of the side effects of introducing modern information technologies in the management of economic, social, organizational and technical systems is the stronger dependence of the management quality on intentional or accidental destructive influences which violate the integrity, confidentiality and availability of the information used. This determines the relevance of developing appropriate information security systems. The substantiation of the development of such systems requires solving the problems of comparative assessment of the destructive impact risks and the cost of their prevention.* ***Purpose:*** *Predicting the danger of a destructive impact on information processes in control systems.* ***Method:*** *The prediction is based on representing the destructive effects in the form of a random sequence of events which lead to disruptions in the information processes. The consequences of failures are also represented by certain random variables.* ***Results:*** *Methodical approaches are proposed in order to build models for predicting temporal and volumetric characteristics of damage from destructive influences on information processes in the management of economic, social, organizational and technical systems. In these models, we suggest to assess the danger of destructive impacts by the probability of the onset of a destructive event at a certain time moment, and by the amount of damage caused by it. The basis for the construction of prediction models is the presentation of damage indicators in the form of step functions of time. The constructive representation of these functions is based on the conditional deterministic approach. The completeness of a priori information usage in determining specific parameters of the damage functions is ensured by applying the maximum uncertainty principle. The measure for the uncertainty is entropy. The conditional deterministic approach for higher uncertainty levels was developed in a stochastic approach. On its basis, classes of stochastic models were proposed, corresponding to various information situations. These models allow you to estimate not only the expected values of damage indicators due to the failure in taking measures to ensure information security while managing targeted systems, but also their probabilistic characteristics.* ***Practical relevance:*** *The proposed approaches are the basis for the creation of particular models and techniques in the interests of well substantiated decisions on the formation of the structure of the organization and management of information security subsystems.*

Keywords — *information systems, information security, destructive impacts, damage, damage prediction models.*

Introduction

The functional success of different goal-oriented systems (economic, social, organizational, technical ones) is defined by the effectiveness of their management. The extent to which the potential resources of these systems are used to achieve goals reflects the effectiveness of their management. It depends on the completeness, reliability and timeliness of information about the current state of a goal-oriented system and the external environment, as well as on the ability of control subsystems to form and realize effective control actions. Therefore, currently information technology is being widely implemented in order to manage these systems effectively.

With modern information technology introduced to the management of economic, social, organizational and technical systems, the quality of management is becoming increasingly dependent on intentional and accidental destructive influences, which violate the integrity, confidentiality and availability of information used [1–6]. So appropriate information security subsystems are created. In order to justify the decisions on the composition of the organization's structure and the operation of such subsystems, the risk must be assessed concerning various destructive influences that affect information processes in the corresponding management systems. The basis of the assessment is projecting the temporal and quantitative characteristics of the damage. This paper proposes methodological approaches which can be used to build conditionally deterministic and stochastic models intended for forecasting these characteristics based on the representation of damage indicators in the

form of jump functions of time. To ensure the most complete use of a priori information when determining the specific parameters of these functions, it is proposed to be guided by the requirements of the maximum uncertainty principle.

Methodical approach to building conditionally determined models for forecasting the risk of destructive influences

When applying the conditionally deterministic approach, the dynamics of damages from the destructive influences exerted on information processes of management systems are simulated using the following relations:

$$x(t) = \sum_{j=1}^{n} a_j n(t - t_j), \qquad (1)$$

where $x(t)$ is the expected value of the selected damage indicator by time t; j is the identifier of the destructive event; n is the number of possible destructive events; a_j is the expected magnitude of the increase in the damage value associated with the destructive event; t_j is the expected time when the destructive event occurs;

$$n(t - t_j) = \begin{cases} 1, \text{ if } (t - t_j) > 0 \\ 0, \text{ if } (t - t_j) \le 0 \end{cases}, j = 1, 2, \dots, n. \qquad (2)$$

Constructive representation of relations (1) requires the definition of the type and specific parameters of functions

$$a_j = f_1(j); \qquad (3)$$

$$t_j = f_2(j). \qquad (4)$$

The initial information for solving this problem is a set of data on the values of x_j, t_j accumulated during the period preceding the forecast, as well as a priori data on the possible nature of the forecasted processes, obtained on the basis of expert assessments and (or) management experience of similar economic, social, organizational and technical systems [7–10].

If the principle of maximum uncertainty is applied, it ensures the completeness of the used information in determining specific parameters of the functions (3), (4). This principle postulates that the least dubious representation of these functions will be one that takes into account all given information and maximizes uncertainty [11].

Such an approach to the construction of the given functions allows us to minimize the impact of subjective assessments and at the same time take into account the full account the available objective information on the conditions of implementation and the characteristics of damage from the destructive influence on information processes in the management systems we study.

The experience of managing various economic, social, organizational and technical systems shows that as they develop and consolidate, the jumps in the values of damage indicators increase due to the occurrence of subsequent destructive events, that is, the following condition is true for the values of function (3)

$$a_n > a_{n-1} > \dots > a_1. \qquad (5)$$

With regard to function (4) we can assume that, if no measures are taken to ensure information security

$$t_1 > t_2 > \dots > t_n, \qquad (6)$$

it is a decreasing function of the integer argument j.

If relations (5) and (6) are true and the values a_j and t_j are independent, the average jump in the damage indicator over the previous operation period of the information system equals a_0, and the average time between destructive impacts during this period is t_0, the ratio (3) can be represented as follows

$$a_j = a_0 F_1(j), j = 1, 2, \dots, n, \qquad (7)$$

where $F_1(j)$ is the corresponding probability functions for the elements in the relation (5).

Function (4) can be represented as

$$t_j = t_0 F_2(j), j = 1, 2, \dots, n, \qquad (8)$$

where $F_2(j)$ is the corresponding probability functions for elements in the relation (6).

The implementation of the maximum uncertainty principle in the definition of functions $F_1(j)$, $F_2(j)$ is ensured by the use of appropriate conditional optimization models [12, 13]. At the same time, in the information situation we consider, it is appropriate to use the second-order entropy to estimate the level of uncertainty

$$H_2(F_2) = \prod_{j=1}^{n} F_2^{n-j+1}(j). \qquad (9)$$

Then the problem model for determining the probability function $F_2(j)$ included in (8) takes the following form [12, 13]:

$$H_2(F_2) = \prod_{j=1}^{n} F_2^{n-j+1}(j) \underset{F_2(j)}{\to} \max; \qquad (10)$$

$$\sum_{j=1}^{n} F_2(j) = 1. \tag{11}$$

Solving this problem with regard to condition (6), we obtain

$$F_2(j) = \frac{n-j+2}{n \cdot 2^j}, \ j = 1, \ 2, \ \ldots, \ n. \tag{12}$$

The functions $F_1(j)$ included in (7) are determined by the relation

$$F_1(j) = 1 - F_2(j), \ j = 1, \ 2, \ \ldots, \ n. \tag{13}$$

If the assumptions about the mandatory increase in the magnitude of jumps in damage indicators for destructive influences can be weakened, then relation (5) takes the form

$$a_n \geq a_{n-1} \geq \ldots \geq a_1. \tag{14}$$

Then the maximum entropy function of the elements probabilities for the variational series (7) has the form

$$F_1(j) = 1 - \frac{2n-j+1}{n(n+1)}, \ j = 1, \ 2, \ \ldots, \ n. \tag{15}$$

If it is appropriate to weaken the assumption that the intensity of destructive influences increases, relation (6) can be represented as

$$t_1 \geq t_2 \geq \ldots \geq t_n. \tag{16}$$

Then the maximum entropy function $F_2(j)$ is determined by the relation

$$F_2(j) = 1 - \frac{2n-j+1}{n(n+1)}, \ j = 1, \ 2, \ \ldots, \ n. \tag{17}$$

Relations (12), (15), (17) were obtained for the first time in [12].

In general, relations (1)–(4), (7), (8), (12), (13) represent a class of conditionally determined forecasting models of jumps in the values of estimated damage indicators from destructive influences exerted on information processes in control systems under the assumptions about the nature of the processes given by relations (5), (6).

Relations (1)–(4), (7), (8), (15), (16) represent a class of conditionally determined forecasting models of jumps in the values of estimated damage indicators from destructive influences on information processes in control systems under the assumptions about the nature of the processes given by relations (5), (14).

Relations (1)–(4), (15), (17) represent a class of conditionally determined forecasting models of jumps in the values of estimated damage indicators under the assumptions set by the relations (14), (16)

Methodical approach to building stochastic forecasting models for the risk of destructive influences

We should note that the conditionally deterministic approach to building forecasting models does not take into account to a full extent the random nature of the results of destructive influence exerted on information processes in management systems. Therefore, along with these models, in some cases it is reasonable to use stochastic models, which allow us to estimate not only the expected values of the corresponding damage indicators, but also their probabilistic characteristics.

In order to build stochastic forecasting models of the danger of destructive influences, the set of values x_j, t_j, which was determined during the period preceding the forecast, should be considered as a sample

$$x_1, \ t_1; \ x_2, \ t_2; \ \ldots; \ x_n, \ t_n \tag{18}$$

of random values of jumps X of the estimated damage indicator and frequency T of their appearance governed by the law of two-dimensional distribution $Q(x, \ t)$ of the population. The possibilities of building various stochastic models are determined by the size of this sample. If the sample size is sufficient to determine only average time $\bar{t}$ between destructive influences

$$\bar{t} = \frac{\sum_{i=1}^{n} t_i}{n} \tag{19}$$

and average damage $\bar{x}$, due to these influences

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n}. \tag{20}$$

Then in such an informational situation there are no objective grounds for assuming random variables T and X to be dependent, and the function of their joint distribution is determined by the relation

$$Q(x, \ t) = W_1(x) W_2(t) \tag{21}$$

and the density function of this distribution is determined by the ratio

$$q(x, \ t) = \frac{\partial W_1(x) W_2(t)}{\partial x \partial t}. \tag{22}$$

In relations (21), (22) $W_1(x)$, $W_2(t)$ are the particular (marginal) distribution functions of the random variables X and T, respectively. At the same time, based on the principle of "maximum uncertainty" in the information situation under consideration, the distributions $W_1(x)$ and $W_2(t)$ can be considered exponential:

$$W_1(x) = 1 - e^{-\frac{1}{\overline{x}}x}; \qquad (23)$$

$$W_2(t) = 1 - e^{-\frac{1}{\overline{t}}t}. \qquad (24)$$

If the sample size is sufficient to determine not only the average time t_0 between destructive influences causing damage and the average value x_0 of the jump in the damage indicator, but also the correlation coefficient r_{xt}:

$$r_{xt} = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(t_i - \overline{t})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2}\sqrt{\sum_{i=1}^{n}(t_i - \overline{t})^2}}, \qquad (25)$$

then the two-dimensional Gumbel distribution [14] is the model for the forecasting of jumps in the damage indicator in accordance with the principle of "maximum uncertainty" when measuring uncertainty using the first-order entropy.

Taking into account the previously adopted notation, the density function of this distribution is

$$q(x, t) = \frac{1}{\overline{x}\overline{t}}\exp\left(\frac{xt}{\overline{x}\overline{t}}\right)\left[1 + \rho\left(2e^{-\frac{x}{\overline{x}}} - 1\right)\left(2e^{-\frac{t}{\overline{t}}} - 1\right)\right]. \qquad (26)$$

The parameter ρ of function (18) is determined by the relation

$$\rho = 4r_{xt}. \qquad (27)$$

But if the sample size (18), along with the mathematical expectations $\overline{x}$, $\overline{t}$, the variances σ_x^2, σ_t^2 and the correlation coefficient r_{xt} of random variables X and T, allows determining the partial laws $W_1(x)$, $W_2(t)$ of their distribution, then the form of the joint distribution function of the random variables under consideration can be refined. Since the available objective information about their joint distribution is only this sample, it is advisable to accept the identity of mathematical expectations, variances and correlation coefficient for the function $q(x, t)$ and the sample (18) as the criterion for the compliance of the function $q(x, t)$ of the real density function of the joint distribution of random variables X and T. In this case, the most appropriate form of function $q(x, t)$ the presentation is the following:

$$q(x, t) = w_1(x)w_2(t)\{1 + \gamma[1 - 2W_1(x)][1 - 2W_2(t)]\}, \qquad (28)$$

where $W_1(x)$ is the partial density distribution function of random variable X; $W_2(t)$ is the partial density distribution function of random variable T; γ is the parameter of the law of joint distribution of random variables X and T.

The density distribution function (28) is a generalization of the function (26), and parameter γ is the linear function of the correlation coefficient:

$$\gamma = r_{xt}J_0[W_1(x), W_2(t)], \qquad (29)$$

where $J_0[W_1(x), W_2(t)]$ is the functional defined by the partial laws $W_1(x)$, $W_2(t)$ of the distribution of random variables X and T.

The value $J_0[W_1(x), W_2(t)]$ is determined by the ratio:

Partial distributions	Distribution density	Distribution function	Distribution parameters		$\dfrac{J_1}{J_2}$	$J_0[W_1(x), W_2(t)]$
			Math. Exp.	Variance		
$W_1(x)$ — exponential $0 < x < \infty$	$w_1(x) = \dfrac{1}{\overline{x}}e^{-\frac{1}{\overline{x}}x}$	$W_1(x) = 1 - e^{-\frac{1}{\overline{x}}x}$	$\overline{x}$	$\overline{x}^2$	$\dfrac{3\overline{x}}{2}$	4
$W_2(t)$ — exponential $0 < t < \infty$	$w_2(t) = \dfrac{1}{\overline{t}}e^{-\frac{1}{\overline{t}}t}$	$W_2(t) = 1 - e^{-\frac{1}{\overline{t}}t}$	$\overline{t}$	$\overline{t}^2$	$\dfrac{3\overline{t}}{2}$	4
$W_1(x)$ — uniform $0 < x < a$	$w_1 = \dfrac{1}{a}$	$W_1(x) = \dfrac{x}{a}$	$\dfrac{a}{2}$	$\dfrac{a^2}{12}$	$\dfrac{2a}{3}$	$\dfrac{6}{\sqrt{3}}$
$W_2(t)$ — exponential $0 < t < \infty$	$w_2(t) = \dfrac{1}{\overline{t}}e^{-\frac{1}{\overline{t}}t}$	$W_2(t) = 1 - e^{-\frac{1}{\overline{t}}t}$	$\overline{t}$	$\overline{t}^2$	$\dfrac{3\overline{t}}{2}$	$\dfrac{6}{\sqrt{3}}$

$$J_0[W_1(x),\, W_2(t)] = \frac{\sigma_x \sigma_t}{(\overline{x} + J_1)(\overline{t} + J_2)}, \qquad (30)$$

where $J_1 = 2\int x w_1(x) W_1(x)\mathrm{d}x;\;\; J_2 = 2\int t w_2(t) W_2(t)\mathrm{d}t.$

The values of parameters J_0, J_1, J_2 for some typical partial laws of distribution of random variables X and T are given in the table.

The integral probability distribution function for the functions (22), (26), (28) is

$$Q(x,\, t) = \int\limits_0^t \int\limits_0^x q(x,\, t)\mathrm{d}x\mathrm{d}t. \qquad (31)$$

Using this function, it is possible to determine the probability that, if no measures are taken to ensure information security during time t, there will be damage of value x.

In general, relations (22), (26), (28), (31) represent a class of stochastic models that allow estimating not only the expected values of damage indicators due to failing to take information security measures when managing goal-oriented systems, but also their probabilistic characteristics.

Conclusion

The widespread adoption of information technology in the management of economic, social, organizational and technical systems and the globalization of information systems are accompanied by the aggravating problem of coping with destructive influences that violate the integrity, confidentiality and availability of information used. Its solution involves the creation of information security subsystems within the framework of information and management systems. Generating informed decisions on their creation and operation is based on predicting the danger of destructive influences on information processes in control systems. The paper proposed methodological approaches to the construction of models of such a forecast. The specific feature of the approaches is the fact that the "maximum uncertainty" principle in the maximum entropy form is used to integrate the available information on the nature of the forecasted processes. This allows us to increase the reliability of the forecast and thereby increase the validity of decisions on the creation and development of the functioning of information security subsystems.

References

1. Garcia-Font V., Garrigues C., Rifà-Pous H. Attack classification schema for smart city WSNs. *Sensors*, 2017, vol. 17, no. 4, p. 771.
2. Perera C., Ranjan R., Wang L., Khan S. U., Zomaya A. Y. Big data privacy in the internet of things era. *IT Professional*, 2015, vol. 17, iss. 3, pp. 32–39.
3. Anisimov V. G., Zegzhda P. D., Anisimov E. G., Bazhin D. A. A Risk-oriented approach to the control arrangement of security protection subsystems of information systems. *Automatic Control and Computer Sciences*, 2016, vol. 50, no. 8, pp. 717–721.
4. Samonas S., Coss D. The CIA strikes back: redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 2014, vol. 10, no. 3, pp. 21–45.
5. Open Group Standard: Open Information Security Management Maturity Model (O-ISM3), Version 2.0. Reading, Berkshire, U. K., The Open Group, 2017. 130 p.
6. Anisimov V. G., Zegzhda P. D., Anisimov E. G., Saurenko T. N., Prisyazhnyuk S. P. Indices of the effectiveness of information protection in an information interaction system for controlling complex distributed organizational objects. *Automatic Control and Computer Sciences*, 2017, vol. 51, no. 8, pp. 824–828.
7. Bertino E., Ferrari E. *Big Data Security and Privacy.* In: *A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years*. Studies in Big Data, Springer, 2018. Vol. 31. Pp. 425–439.
8. Anisimov V. G., Anisimov E. G., Saurenko T. N., Sonkin M. A. The Model and the planning method of volume and variety assessment of innovative products in an industrial enterprise. *Journal of Physics: Conference Series*, 2017, vol. 803, no. 1, p. 012006. doi: org/10.1088/1742-6596/803/1/012006
9. Akeel F., et al. Formal modelling of data integration systems security policies. *Data Science and Engineering*, 2016, vol. 1, iss. 3, pp. 139–148. doi:10.1007/s41019-016-0016
10. Anisimov V., Anisimov E., Sonkin M. A Resource-and-time method to optimize the performance of several interrelated operations. *International Journal of Applied Engineering Research*, 2015, vol. 10, no. 17, pp. 38127–38132.
11. *Jaynes E. T.* Information theory and statistical mechanics. *Physical Review. Series II*, 1957, vol. 106, no. 4, pp. 620–630.
12. Fishburn Peter C. *Nonlinear Preference and Utility Theory*. Baltimore, Md., Johns Hopkins University Press, 1988. 259 p.
13. Saurenko T., Anisimov E., Anisimov V., Levina A. Comparing investment projects of innovative developing strategies of municipalities, based on a set of indicators. *MATEC Web of Conferences "International Science Conference SPbWOSCE-2017 "Business Technologies for Sustainable Urban Development"*, 2018, p. 01038.
14. Gumbel E. J. *Statistical theory of extreme values and some practical applications*. Applied Mathematics Series. 33. 1st ed. U. S., Department of Commerce, National Bureau of Standards, 1954. 60 p.

Модели прогнозирования опасности деструктивных воздействий на информационные процессы в системах управления

В. Г. Анисимов[а], доктор техн. наук, профессор, orcid.org/ 0000-0002-5097-4618, an-33@yandex.ru

Е. Г. Анисимов[б], доктор техн. наук, профессор, orcid.org/ 0000-0002-6527-2352

Т. Н. Сауренко[б], доктор экон. наук, заведующий кафедрой, orcid.org/ 0000-0003-1736-7178

Е. А. Зотова[а], ассистент, orcid.org/ 0000-0003-4539-4253

[а]Санкт-Петербургский политехнический университет Петра Великого, Политехническая ул., 29, Санкт-Петербург, 195251, РФ

[б]Российский университет дружбы народов, Миклухо-Маклая ул., 6, Москва, 117198, РФ

Введение: одним из побочных эффектов внедрения современных информационных технологий в управление экономическими, социальными, организационно-техническими и техническими системами является обострение зависимости качества управления от преднамеренных и случайных деструктивных воздействий, нарушающих целостность, конфиденциальность и доступность используемой информации. Это определяет актуальность развития соответствующих систем обеспечения информационной безопасности. Обоснование путей развития таких систем требует решения проблем сравнительной оценки опасности соответствующих деструктивных воздействий и затрат на их предотвращение. **Цель исследования:** прогнозирование опасности деструктивных воздействий на информационные процессы в системах управления. **Методы:** представление деструктивных воздействий в виде случайной последовательности событий, приводящих к сбоям информационных процессов. Последствия сбоев также представляются соответствующими случайными величинами. **Результаты:** предложены методические подходы к построению моделей прогнозирования временных и объемных характеристик ущербов в форме скачкообразных функций на информационные процессы в системах управления экономическими, социальными, организационно-техническими и техническими системами. В этих моделях опасность указанных деструктивных воздействий предлагается оценивать вероятностью наступления в некоторый момент времени деструктивного события и обусловленной им величиной ущерба. В основу построения моделей прогнозирования положено представление показателей ущербов в форме скачкообразных функций от времени. В основу конструктивного представления этих функций положен условно-детерминистический подход. Полнота использования априорной информации при определении конкретных параметров функций ущерба обеспечивается применением принципа максимума неопределенности. Мерой неопределенности принята энтропия. Развитием условно-детерминистического подхода для более высоких уровней неопределенности явился стохастический подход. На его основе предложены соответствующие различным информационным ситуациям классы стохастических моделей, позволяющих оценивать не только ожидаемые величины показателей ущербов вследствие непринятия мер обеспечения информационной безопасности при управлении целенаправленными системами, но и их вероятностные характеристики. **Практическая значимость:** предлагаемые подходы являются базой для создания конкретных моделей и методик в интересах обоснования решений по формированию состава структуры организации и управления функционированием подсистем обеспечения информационной безопасности.

Ключевые слова — информационные системы, информационная безопасность, деструктивные воздействия, ущерб, модели прогнозирования ущерба.

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, снижая рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12-ти языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org