Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2018, №1, Том 10 / 2018, No 1, Vol 10 https://esj.today/issue-1-2018.html

URL статьи: https://esj.today/PDF/25ECAVN118.pdf

Статья поступила в редакцию 03.03.2018; опубликована 24.04.2018

Ссылка для цитирования этой статьи:
Диалло А.Б., Дим Д.Т., Бакасов С.Р., Богатиков В.Н. Использование «метода уступок» при выборе оптимального варианта защиты корпоративной сети // Вестник Евразийской науки, 2018 №1, https://esj.today/PDF/25ECAVN118.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

For citation:
Diallo A.B., Dim D.T., Bakasov S.R., Bogatikov V.N. (2018). Implementing "method of successive concessions" in selecting the optimal variant to protect a corporate network. *The Eurasian Scientific Journal*, [online] 1(10). Available at: https://esj.today/PDF/25ECAVN118.pdf (in Russian)

Российский Фонд Фундаментальных Исследований (РФФИ) «Исследование рисков при управлении динамическими процессами в слабоструктурированных и плохо формализуемых средах», проект № 17-07-01368

The work was carried out with the financial support of RFBR grant «Risk study in the management of dynamic processes in semi-structured and poorly formalized environments», Project № 17-07-01368

Diallo Amadou Bhoye
Tver state technical university, Tver, Russia
E-mail: amsbhoye@yahoo.fr

Dim Dike Terfa
Tver state technical university, Tver, Russia
E-mail: dt_dim@mail.ru

Bakasov Sabir Rumovich
Tver state technical university, Tver, Russia
E-mail: sabir17204@gmail.com

Bogatikov Valerij Nikolaevich
Tver state technical university, Tver, Russia
E-mail: VNBGTK@mail.ru

Implementing "method of successive concessions" in selecting the optimal variant to protect a corporate network

Abstract. The choice of software and hardware products for information protection against a variety of threats that arises in enterprise network systems are currently a serious problem due to the high requirements in stability of network operations and information security.

In this paper, selection of an optimal variant for corporate networks is considered. A method of concessions is proposed to solve this problem.

A method of concessions to solve this problem is proposed. Method of successive concessions in choosing the optimal protection system. As already mentioned, the method involves the multi criteria optimization problem to the single-criteria. It represents an iterative human-machine procedure which when used, the developer gives permissible increments of one parameters (particularly, by setting a reduction in the security coefficient), analyzes the change of others by deciding on the admissibility of inputs. In this paper, consideration is offered for a step-by-step method of evaluating the Information Protection system and choosing the optimal variant for the protection system (the necessary set of protection mechanisms).

Parameters with which the method operates, ways of obtaining them and their estimation are described. Description of the information system is recommended in accordance with the following plan: hardware, their configuration, software used, interface of the system, i.e. external and internal connections from the position Information technology. Personnel working on this information system, architecture of the security subsystem, software and hardware to provide information security, etc.

Keywords: information security; corporate networks; analysis method; method of concessions; information safety; information risk; risk management

Method of successive concessions is an iterative human-machine procedure, in which the developer by permissible increments of one parameter (particularly, by specifying the reduction of security coefficient), analyzes the change in others, deciding on admissibility of the concessions [8].

In method of concessions, the decision-maker chooses the task, gradually weakening initial requirements that are generally impossible to be fulfilled at the same time [9]. The sequence of getting the solution is as follows:

- find the maximum value Z_1^* of the first criterion $Z = Z_1(x)$ on all acceptable solutions;
- determine the value of permissible concessions reduction D_1 of criteria $Z_1(x)$ and find the highest value Z_2^* of the second criterion $Z = Z_2(x)$, provided that the value of the first criterion is not less $Z_1^* - D_1$.

Next is to determine the amount of permissible reduction concessions D_2 criterion $Z_2(x)$ and look for the greatest value Z_3^* of the third criterion $Z = Z_3(x)$ at the same time, that the value of the second criterion should not be less etc.

A qualitative analysis of the relative significance of the criteria is first made to determine the value of concessions. Based on this analysis, the criteria are listed in order to reduce their importance.

The size of concessions characterizes the difference in priority of certain criteria with respect to other criteria. From the lexicographical point of view, criteria classification: the less concessions, the more difficult the priority.

As such, the optimal solution is any solution of the multi-criteria problem of the last task of the sequence [10]:

a) Find $\max Z_1(x) = Z_1^*$ in the area $x \in X$;

b) Find $\max Z_2(x) = Z_2^*$ in the area defined by the terms

$$x \in X \; ; \; Z_1(x) \geq Z_1^* - D_1 \; ; \qquad (1)$$

c) Find $\max Z_m(x) = Z_m^*$ in the area defined by the conditions $x \in X$; $Z_1(x) \geq Z_1^* - D_1$, $i = 1, ..., m-1$;

The optimum is usually considered as the last solution obtained from the previously assigned set of selected criteria [8]. The problem is reduced to a sequence of tasks for calculating the extrema of a particular criterion, with a consequent reduction by a certain value called concession. This simplifies the solution in many ways but gives an approximate result.

Method of successive concessions does not necessarily lead to obtaining effective points, there is always at least one effective point between these points. This has the following claims.

Proposition 1. If $X \subset R^n$ is a closed and limited set, and the functions Z_i are continuous, then at least one effective point is obtained by the solution of M-th problem (1).

Proposition 2. If x^* the only point (until equivalence) that is the solution of the M-th task from (1), then it is effective.

Example. By method of successive concessions, find the solution to the problem, assuming that the criteria are ordered sequentially according to importance

$$\{Z_2, Z_1\}, \text{ and } D_2 = 1.$$

$$F(x) = \{Z_1 = -x_1 + 3x_2, Z_2 = 4x_1 - x_2\} \to \max,$$

$$Z_1 = -x_1 + 3x_2 \to \max,\ Z_2(x) = 4x_1 - x_2 \to \max,$$

The first task in sequence:

$$Z_2(x) = 4x_1 - x_2 \to \max,$$

$$\begin{cases} -x_1 + x_2 \le 1 \\ x_1 + x_2 \ge 3 \\ x_1 - 2x_2 \le 0 \\ x_1 \le 4 \\ x_2 \le 3 \end{cases}$$

Solution: $x_1 = 4,\ x_2 = 2,\ Z_1 = 14$

Next we solve the following problem:

$$Z_1 = -x_1 + 3x_2 \to \max$$

$$\begin{cases} -x_1 + x_2 \le 1 \\ x_1 + x_2 \ge 3 \\ x_1 - 2x_2 \le 0 \\ x_1 \le 4 \\ x_2 \le 3 \end{cases}$$

$$4x_1 - x_2 \ge 13$$

In this case, using the solution of the first problem and the value concessions $D_2 = 1$, we introduce an additional restriction $4x_1 - x_2 \ge 13$. From this solution we get the following optimal plan: $x_1 = 4,\ x_2 = 3,\ Z_2 = 5,\ Z_1 = 13.$

Fig. 1 shows qualitative dependence of change in the main parameters characterizing system protection, from its complexity-the set of protection mechanisms. It is clearly visible from the graph that the cost of information protection (*IP*) of a complex system increases unlimitedly and the productivity is decreases in the limit to zero.

25ECAVN118
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

At the same time, the security coefficient curve (*D, fig. 1*) tends to the limiting value – *(100 %)* and reaches saturation. Simultaneous with a further increase in complexity (and subsequent increase in price, as well as decrease in productivity), the increase in security coefficient is insignificant.

Therefore, when designing an *IPS*, it is expedient to analyze other values of the security parameters from the saturation region. In other words, it is advisable to investigate the possibility of using less complex security systems and by setting a certain interval of reducing the security coefficient (*ΔD*), select a system whose security level satisfies the value of (*D-ΔD*).

This can result in a tangible price and productivity gain [5].

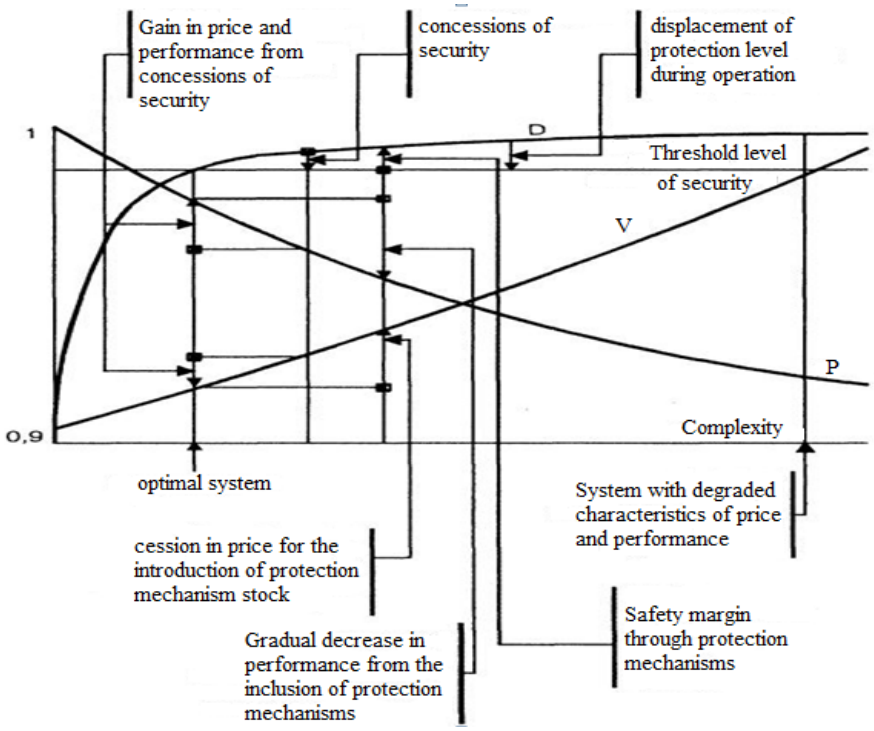

Figure 1. *Application for method of consecutive concessions*
Рисунок 1. *Иллюстрация применения метода последовательных уступок*

This application is a known method of successive concessions, which can be applied to optimize the protection system and as previously mentioned, is associated with reducing the complexity of multi-criteria optimization task to the level of complexity single criterion.

When analyzing an information system's level of security, we distinguish the following: receipt of raw data, analysis. Based on the analysis, decisions are made to improve the parameters of the protection system.

In this work, the functionality of system security (Z) is determined depending on the cost of protected information, the level of the possibility of hacking, complexity and, accordingly, the cost of protection system, as well as the performance of information system.

In this paper, functionality of a system security (*Z*) is determined based on the cost of the protected information, probability of penetration, cost of the security system and system performance:

$$Z = f(S_{INF}, P_P, C_{IPS}, P_{IPS})$$

Where:

S_{INF} – Cost of the protected information;

P_P – probability of penetration;

25ECAVN118
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

C_{IPS} – Cost of *IPS*;

P_{IPS} – *IPS* performance.

Evaluation of security based on the above calculation formulas and the choice of the optimal variant for the information protection system (the necessary set of protection mechanisms) is carried out as follows [4]:

1. Calculation of parameters C_i, λ_i, P_i (P_i – probability of reflection of protection system's i-th threats, C_i – cost of loss from protection breach i-type, accordingly). If the research data is not available, assessing safety based on, for example, expert assessment methods.
2. Calculation of the security criteria for each version of the protection system (a set of protection mechanisms) D, C_{IPS}, P_{IPS} (δP_{ISP}). Where D – safety coefficient; (δP_{ISP}) – decreased performance of the information system's protection.
3. Selecting a set of protection mechanisms and means of their implementation during development with maximum protection coefficient D, satisfying the cost constraints of the C_{IPS} and the performance of P_{IPS}.
4. Analysis of the change in the protection coefficient δD when setting increments for the C_{IPS} and δP_{IPS} criteria by the method of sequential selection of concessions with an assessment of the expediency of selecting a system that meets the new constraints.

When designing information security systems, the most relevant research section is the formation of requirements for obtaining accurate data close to reality and more relevant to the specifics of the organization, and therefore, at the preparatory stage, a detailed description of the system is required. The importance of a preliminary study when creating safety management systems for the formation of requirements is obviously because, the better the expert knows the object, the more accurate the protection estimate [7].

Considering the purposes of creating an information system, limitation of its information resources, level of information security requirements, components of the information management system and information security regime, a strategy is formed creating the protection system [1, 3]. Based on the formed goals in the construction of the system, the following tasks are solved:

- Hardware selection and configuration;
- Software selection;
- Design of system interface, which clearly define the interconnections of physical system objects, their external and internal data flows from information technology standpoint;
- Identification of data types and information;
- Formation of personnel working on this information system;
- Identification of the information system's mission (main objectives). At different stages the objectives can be modified and refined;
- Determining critical data types and information processes;
- Forming and refining functionality requirements to the information system in the process of project creation;
- Definition of the system user's category;
- Formation of formal requirements for information security, applicable to this security system of a particular organization (legislation, departmental standards and so on);

- Design of information security subsystem architecture and topology of the corporate network;
- Design of software and hardware configuration to provide information security;
- Organization of input and output data streams;
- Designing the management system of the information security organizational structure (Information security planning system, job descriptions);
- Modernization of the information system's security management (secure copying, emergency response to possible attacks from external environment, information security control maintenance, instruction in information security and so on);
- Design for the newly created physical system of security organization;
- Modernizing the management and control of the Information security environment (climatic parameters, power supply, flood protection, aggressive environment and so on).

To assess the cost of the information security system, the following work options are performed:

1. Collection and synthesis of materials, scientific research, in the process that defines the necessary tools, used in practice for calculating indicators and security measures. The results include the management of the company to assess the value of protected data and determine the likelihood of potential attacks and possibly existing vulnerabilities, as well as the level of potential damage. Where the information costs nothing, there are no significant threats to the company's information assets and the potential damage is minimal. Leadership then concurs and waves off the need to deal with the information security problem. If the information is worth a certain amount of money, threats and potential damage are clear, then the budget framework for the corporate information security system is also understandable. It is essential that to draw company management's attention as soon as possible to IS problems and to build a corporate information security system that enlist its support. As such this approach for assessing the cost of a security system can be used without imposing restrictions on the C_{IPS} parameter but only on the required level of security [6].

2. Another option to increase protection against possible attacks that could lead to violations of data protection of corporate enterprises or organizations is the choice of a finished product or the use of ready-made means of information security. i. e. searching for the invariant value of the information security system. In reality, there are similar systems for other businesses or organizations that can be migrated to the enterprise with the appropriate hardware and software.

As a result of research, experts in the field of information protection found some optimum, which provides relative confidence that the cost of information security system should be approximately 10-20 % of the cost of corporate Information systems depending on the level of information confidentiality. The application of this assessment leads to positive results in practice, which can be relied upon. Obviously, the second stage is not without shortcomings. It is most likely impossible to force the management to realize the depth of information security problems. But it creates an opportunity to build the initial judgement, based on this judgement, it is possible to predict the volume of the budget for the security information system and significantly save on the services of external consultants [2].

The selection of an effective system in any field should be characterized by some parameters that constitute the selection basis. You can select the following options for the information security system: manageability, cost, compatibility, performance, security, and more. The use of classical methods to determine the extrema for the implementation of procedures in selection of security

characteristics is not always an effective way to solve due to the complexity problems in synthesis of systems, which are information security systems.

In addition, a lot of conflicting parameters: with increase in security level, for example, cost increases, as well as the complexity of the configuration but at the same time performance decreases. This method will therefore assess the effectiveness of the system with respect to the security setting. This is due to the fact that the main indicator characterizes the level of protection provided by the information protection system. While other parameters and characteristics are subject to limitations.

Quite often in the periodical literature the choice of the best variant of the information protection system which is based on the criterion of competitiveness of the enterprise is offered. Based on this conclusion, for example, the authors [11] seek to improve the state of protection of the enterprise against threats to information security.

The theoretical value for the coefficient of change in competitiveness based on the coefficient of relative loss reduction after introducing an improved version of the information protection system (IPS) is obtained in the paper. By predicting and analyzing of the coefficient of relative damage reduction for various types of external attacks, the most rational system of organization protection is chosen. Randomization method was used to find the best solution. On one hand, the method gives an approximate solution but at the same time it allows for the selection of the IPS structure variant quickly enough. The application of this IPS model increases the state of information protection of an industrial enterprise and organization.

In paper [12] the problem of choosing a rational composition of information protection system in a holding's multifunctional information system was considered. Method of competing systems by categories of processed information is proposed. Also substantiated, is the necessity of using the method of morphological synthesis of the software and hardware complex of information protection. This method allows to implement a multi-criteria and multi-alternative choice. A methodology for the synthesis of a rational software and hardware information protection complex was developed.

The choice of network tools for information protection, implementing the policy of information security, is an important stage in the process of information security policy Management. In this paper the peculiarities and shortcomings of the existing network tools selection method of information protection are considered, as well as the method of choosing network tools for information protection, taking into account the cost of network tools for Information protection [13].

In paper [14] the object security model is based on the relationship between the elements of multiple leakage channels K = {K1, K2, …, Km} and a set of protection means S = {S_1, S_2, …, S_n}. The interconnection of sets is easy and convenient to present in the form of a bipartite graph, where the edges of the graph correspond to the relationship between leakage channels and the means of protection. The links have two parameters: the cost of C = {C_{11}, …, C_{mn}} and the efficiency coefficient Ef = {Ef_{11}, …, Ef_{mn}} effective use of protection as an active means of ensuring information security. Efficiency is determined by expert assessments.

Taking into account the properties of the model based on relationship of sets, which can be represented as a bipartite graph, the task of searching for the IPS variant is considered as two problems of conditional optimization based on the algorithm of maximal matching construction: Maximize the efficiency (Ef -> max) for a given budget (C = const) and the problem of finding a variant of the IPS with a minimum cost (C -> min) for a given efficiency (Ef = const).

Proposed in [15] is the process of creating and managing security policy based on the Six Sigma model and is a way to adapt the security objectives and risk management of the compute service. formalizing the process of managing security policy within the industrial process model, the adaptability of this model to existing industrial software offers a clear strategy for risk-based decision-making. In particular, the present document provides the necessary tools and procedures for comparing

the Six Sigma DMAIC (Define-Measure-Analyze-Improve-control) method in the management of security policy.

The method offered in the work is different from those discussed above. For example, [11, 12, 13, 14, 15]. The advantage of the method of successive concessions is that it easily allows you to control by the price, what concessions in one private criterion gains in another private criteria is acquired. It may be noted that the freedom to choose a solution, which is acquired by the price of even minor concessions can be significant because in the vicinity of the minimum, the efficiency of decisions usually varies little.

Other positive qualities of the method of trial and concessions are the availability, low labor input in comparison with other methods. Convenience for practical use.

Despite the ideological simplicity of the method of successive concessions, the practical application of this method is fraught with certain difficulties. It is applicable to solving those multi-criteria optimization tasks in which all private criteria are naturally ordered by the degree of importance.

Conclusion

In this work, a step-by-step method for evaluating the information protection system and successive concessions methods is proposed. The parameters with which the method works, methods of obtaining and their estimation, principles of risk assessment when using this method are all considered.

REFERENCES

1. L. Hmelev. Evaluation of the effectiveness of security measures, laid down in the design of electronic information systems. Proceedings of the scientific and technical conference "Information Technology Security", Penza, June 2001. P. 56-60. URL: http://lib2.znate.ru/docs/index-308561.html?page=10 (Date accessed 25.03.2018).
2. Galickij A. Information protection in networks-analysis of technologies and synthesis of solutions. DMK. 2004. URL: https://vuzlit.ru/983812/opisanie_ poshagovoy_metodiki (Date accessed 25.03.2018).
3. International Standard ISO 17799:2000 "practical rules of information security management" URL: https://www.kazedu.kz/referat/131693/15 (Date accessed25.03.2018).
4. Shheglov A.Ju. Security of computing systems and networks URL: https://studfiles.net/preview/6071060/page:4/ (Date accessed25.03.2018).
5. Petrov Je.G. «Methods and means of decision-making in social economic and technical systems». – Herson: OLDI-Plus, 2003. URL: http://topref.ru/referat/53611.html (Date accessed 25.03.2018).
6. Petrenko S.A., Simonov S.V. Information risk management. Economically justified security. – M.: Kompanija Ajti; DMK Press, 2004. URL: http://studbooks.net/2172360/informatika/metod_ustupok_vybore_optimalnog (Date accessed 25.03.2018).

7. NIST 800-30 стандарт США «Предотвращение и мониторинг инцидентов связанных с вредоносным ПО» URL: https://www.kazedu.kz/referat/131693/17 (Date accessed 25.03.2018).
8. Stoyer R. Multi-criteria optimization / Stoyer R.: translated from English. – M.: Radio and communications, 1992. – 504 p. – (Theory, calculations and applications). https://studfiles.net/preview/4031478/page:4/ (Date accessed 25.03.2018).
9. Podinovskij V.V., Pareto-optimal solutions of multicriteria problems. Podinovskij, V.D. Nogin. – M: Nauka, 1982 – 64 p. URL: http://zazdoc.ru/docs/100/index-155840.html (Date accessed 25.03.2018).
10. Podinovskij V.V., Gavrilov V.M. Optimization by consistently applied criteria. – M: Sov. Radio, 1975. 192 p. URL: http://sfedu.ru/www/umr_main.umr_download?p_umr_id=44983 (Date accessed 25.03.2018).
11. Popova E.V. Choice of the system of information protection according to the criterion of ensuring enterprise competitiveness URL: https://cyberleninka.ru/article/v/ (Date accessed 25.03.2018).
12. Miheev V.A. URL: https://cyberleninka.ru/article/v/metodika-vybora-ratsionalnogo-kompleksa-programmno-apparatnyh-sredstv-zaschity-informatsii-mnogofunktsionalnoy-informatsionnoy (Date accessed 25.03.2018).
13. Chernjavskij D.S. Methods of selection of network means of information protection in accordance with information security policies URL: https://bit.mephi.ru/index.php/bit/article/view/208. (Date accessed 25.03.2018).
14. Podsuhin L.D., Bejsova N.V. Modeling of complex of protection of object of computer equipment from information leakage URL: https://www.s-konsalt.ru/articles/ (Date accessed 25.03.2018).
15. Rees J., Bandyopadhyay S., Spafford E.H. PFIRES: A Policy Framework for Information Security // URL: https://bit.mephi.ru/index.php/bit/article/view/208. (Date accessed 25.03.2018).

УДК 330:001.895

Диалло Амаду Бойе
ФГБОУ ВПО «Тверской государственный технический университет», Тверь, Россия
Аспирант
E-mail: amsbhoye@yahoo.fr

Дим Дике Терфа
ФГБОУ ВПО «Тверской государственный технический университет», Тверь, Россия
Аспирант
E-mail: dt_dim@mail.ru
РИНЦ: https://elibrary.ru/author_profile.asp?id=473456

Бакасов Сабир Румович
ФГБОУ ВПО «Тверской государственный технический университет», Тверь, Россия
Аспирант
E-mail: sabir17204@gmail.com

Богатиков Валерий Николаевич
ФГБОУ ВПО «Тверской государственный технический университет», Тверь, Россия
Доктор технических наук, профессор
E-mail: VNBGTK@mail.ru
РИНЦ: https://elibrary.ru/author_profile.asp?id=8650

Использование «метода уступок» при выборе оптимального варианта защиты корпоративной сети

Аннотация. Выбор программных и аппаратных продуктов для защиты информации от множества угроз, возникающих в корпоративных сетевых системах, в настоящее время является серьезной проблемой из-за высоких требований к стабильности сетевых операций и информационной безопасности. В данной статье рассматривается выбор оптимального варианта для корпоративных сетей. Предлагается метод уступок для решения этой проблемы. Выбрав оптимальные системы защиты, имеется метод последовательных уступок. Как уже ранее говорилось, метод включает проблему многокритериальной оптимизации к однокритериальной и представляет собой итерационную человеко-машинную процедуру, которая при использовании проявителя дает допустимые приращения одного параметра (в частности, путем уменьшения коэффициента безопасности), анализирует модификацию других, принимает решение о допустимости входных данных. В этой работе предлагается рассмотреть поэтапный метод оценки системы защиты информации и системы защиты, которая имеет выбор оптимального варианта (нужный набор механизмов защиты). Описаны параметры, с которыми работает методика, способы их получения и оценка. Рекомендация в соответствии со следующим планом описания информационной системы: аппаратное обеспечение, его конфигурацию, используемое программное обеспечение, интерфейс системы, то есть внешние и внутренние соединения с информационной технологии положении, персонал, работающий над этой информационной системой, архитектура подсистемы информационной безопасности, программное обеспечение и оборудование для обеспечения информационной безопасности и так далее.

Ключевые слова: защита информаций; корпоративная сеть; метод анализа; метод уступок; информационная безопасность; информационный риск; риск-менеджмент

ЛИТЕРАТУРА

1. Л. Хмелев. Оценка эффективности мер безопасности, закладываемых при проектировании электронно-информационных систем. Труды научно-технической конференции "Безопасность информационных технологий", Пенза, июнь 2001. – С. 56-60. [Электронный ресурс] http://lib2.znate.ru/docs/index-308561.html?page=10 (дата обращения 25.03.2018).
2. Галицкий А. Защита информации в сети – анализ технологий и синтез решений. ДМК. 2004. [Электронный ресурс] https://vuzlit.ru/983812/opisanie_poshagovoy_metodiki (дата обращения 25.03.2018).
3. Международный стандарт ISO 17799:2000 “Практические правила управления информационной безопасностью” [Электронный ресурс] https://www.kazedu.kz/referat/131693/15 (дата обращения 25.03.2018).
4. А.Ю. Щеглов безопасность вычислительных систем и сетей [Электронный ресурс] https://studfiles.net/preview/6071060/page:4/ (дата обращения 25.03.2018).
5. Петров Э.Г. «Методы и средства принятия решений в социально экономических и технических системах». – Херсон: ОЛДИ-плюс, 2003. [Электронный ресурс] http://topref.ru/referat/53611.html (дата обращения 25.03.2018).
6. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания Айти; ДМК Пресс, 2004. [Электронный ресурс] http://studbooks.net/2172360/informatika/metod_ustupok_vybore_optimalnog (дата обращения 25.03.2018).
7. NIST 800-30 стандарт США «Предотвращение и мониторинг инцидентов связанных с вредоносным ПО» [Электронный ресурс] https://www.kazedu.kz/referat/131693/17 (дата обращения 25.03.2018).
8. Штойер Р. Многокритериальная оптимизация / Штойер Р.: пер. с англ. – М.: Радио и связь, 1992. – 504 с. – (Теория, вычисления и приложения) https://studfiles.net/preview/4031478/page:4/ (дата обращения 25.03.2018).
9. Подиновский В.В. Парето-оптимальные решения многокритериальных задач / В.В. Подиновский, В.Д. Ногин. – М.: Наука, 1982. – 64 с. [Электронный ресурс] http://zazdoc.ru/docs/100/index-155840.html (дата обращения 25.03.2018).
10. Подиновский В.В., Гаврилов В.М. Оптимизация по последовательно применяемым критериям. – М.: Сов. Радио, 1975, 192 стр. [Электронный ресурс] http://sfedu.ru/www/umr_main.umr_download?p_umr_id=44983 (дата обращения 25.03.2018).
11. Попова Е.В. Выбор варианта системы защиты информации по критерию обеспечения конкурентоспособности предприятия [Электронный ресурс] https://cyberleninka.ru/article/v/ (дата обращения 25.03.2018).
12. В.А. Михеев [Электронный ресурс] https://cyberleninka.ru/article/v/metodika-vybora-ratsionalnogo-kompleksa-programmno-apparatnyh-sredstv-zaschity-informatsii-mnogofunktsionalnoy-informatsionnoy (дата обращения 25.03.2018).
13. Дмитрий Сергеевич Чернявский Методы выбора сетевых средств защиты информации в соответствии с политиками информационной безопасности [Электронный ресурс] https://bit.mephi.ru/index.php/bit/article/view/208 (дата обращения 25.03.2018).
14. Л.Д. Подсухин, Бейсова Н.В. Моделирование комплекса защиты объекта вычислительной техники от утечки информации [Электронный ресурс] https://www.s-konsalt.ru/articles/ (дата обращения 25.03.2018).
15. Rees J., Bandyopadhyay S., Spafford E.H. PFIRES: A Policy Framework for Information Security // [Электронный ресурс] https://bit.mephi.ru/index.php/bit/article/view/208 (дата обращения 25.03.2018).