Study of the effectiveness of combinatorial protection algorithms based on the hardware and software of the electronic storage of corporate information systems

Timofey Asmolov and Rinat Galin
V.A. Trapeznikov Institute of Control Sciences of Russia Academy of Sciences, 65 Profsoyuznaya Street, Moscow, 117997, Russia

E-mail: rinat.r.galin@yandex.ru

Abstract. The paper presents experimental studies of combinatorial algorithms designed to calculate the composition and order of application of vulnerability parry tools, conducted on the basis of a typical electronic repository of the cultural institution information system. Experimental studies of data protection algorithms with the use of a neural network composition calculation unit and the order of application of vulnerability parry tools have been carried out. The proposed approach makes it possible to obtain a gain in time and efficiency (reliability) by using standard means of protecting software tools of large-scale electronic repositories, typical for large cultural institutions.

1. Introduction
The algorithms under study are based on the hypothesis that the impact on the corporate information system containing electronic storage will be carried out in accordance with the strategy that provides conditions for: 1) the shortest way to implement a single vulnerability in the space of pairwise probabilistic connections between them, or 2) multifactorial simultaneous exposure to multiple attacks. The simulation results of the graph representation of the network interacting structures were obtained using self-organizing and dynamic artificial neural networks. A protected information system means a distributed corporate information system (with electronic storage included in it) allowing to save and use heterogeneous collections of electronic documents (text, graphics, audio, video, etc.) that are accessible in a user-friendly form via global data transfer networks [1-4].

2. The structure of the protected objects
To protect the information systems of cultural institutions, an integrated approach is being developed that implements the process of dynamic use of various protection mechanisms from a specific and limited list of means. The general scheme of the corporate information system, which is based on electronic storage, is shown in figure 1 [5-7]. Analysis of the hardware and software features of real corporate information systems with electronic storage enabled showed the diversity of the composition and functions performed related to providing electronic storage processes, which in its turn entails a variety and number of potential vulnerabilities of these systems.
The block diagram of the neural network dynamic calculation for the protection of electronic storage as part of a corporate information system is presented in figure 2.

3. The structure of the neural network computing module
The main functional module of the neural network computing unit of the composition and order of application of vulnerability parry tools is a software/hardware algorithm for the dynamics of the Hopfield neural network and Kohonen map.

Experimental research of algorithms using a neural network computing unit for calculating and applying the tools for countering vulnerabilities of electronic repositories was carried out in comparison with traditional approaches based on a corporate typical information system with an integrated electronic archive and with two high-performance MSSQL DBMS and Oracle with WEB access. Traditional methods of ensuring information security include the application (according to experts of database administrators) strictly - specific protection mechanisms, and their replacement by teams of the same experts. The main security mechanism is the access list, which allows flexible and at the same time simple distribution of rights up to individual attributes. The server audit used in this corporate information system allows to know who carried out specific actions and from what place they were carried out. An administrator or security officer may learn such things as navigating through
the structure of the archive, not to mention viewing and modifying objects, but this takes time, during which the implementation of a particular vulnerability happens.

To speed up operations, using the procedures of combinatorial brute force protection mechanisms or brute force to implement some vulnerability, a neural network parallel computational basis is used.

Figure 3 shows the general flowchart of the neural network calculation algorithm for the composition and procedure of applying the means of countering vulnerabilities in an information system containing an electronic repository. The first three steps form the initial data of the algorithm [8-12].

**Figure 3.** The block diagram of the algorithm of the neural network calculation to the composition and use of means of countering vulnerabilities of information systems based on dynamic neural network.

**Step 1.** At the first step, \(Z\) number of launches of the neural network relaxation is set to its energy minimum.

**Step 2.** At the second step, on the basis of statistical, dynamic internal and dynamic external factors, the vector of recognition of vulnerability implementations is formed by the actions of users of electronic storage: \(v_{i}, i = 1, ..., N\). Since there are much more \(v_{i}\) vulnerabilities than \(d_{j}\) parry tools, vulnerabilities are combinatorially grouped into all possible combinations without repetitions, and each grouping is accepted as a destination unit.

**Step 3.** According to the implementation of the third step, an unordered part of the set of means for countering the implementations of vulnerabilities \(d_{j}, j = 1, ..., M\) is selected.

**Step 4.** At the fourth step, table \(X = \left\| x_{ji} \right\|\) is created to match the set of \(D\) means for countering the implementations of vulnerabilities to \(V\) set of recognized implementations of vulnerabilities by the actions of users of the electronic repository. The table defines the initial data for solving the problem of protecting the electronic storage in the framework of the combinatorial assignment problem.

**Step 5.** The fifth step determines the structure of the neural network model - the type of \(f(s)\) activation function, \(N \times N\) number of neurons, depending on the dimension of the original data vectors and the mode of operation (asynchronous).

**Step 6.** On the sixth step, the coefficients of \(T_{ji}, \mu\) interneuronal connections and \(I_{ji}\) Hopfield neural network model are calculated: \(u = f(u, I, T)\), where \(u\) are the outputs of the neuron, \(I\) are the displacement values, \(T\) are the coefficients of the synoptic connections.
Step 7. The seventh step implements the initialization of the neural network with \( u^0 \) random input vector, as a result of subsequent iterations of which the neural network is set to \( u_{c+1} = f(u_c, I_k, T_k) \) equilibrium state.

Step 8. At the eighth step, an unambiguous interpretation of the output signals of the Hopfield neural network neurons is carried out. Interpretation of the outputs of the neural network allows to get the desired sequence of parrying means in accordance with a given set of implementations of vulnerabilities on the \( r \)–th launch of the neural network.

Step 7-10. Steps from the seventh to the ninth are performed after reaching \( Z \) predetermined number of neural network relaxation launches to its energy minimum (checking \( r \geq Z \) condition at the ninth step).

4. Results of experimental studies

Figures 4-5 show the results of experimental studies of the neural network computing unit and the procedure of applying means to counter the vulnerabilities of electronic storage in accordance with the scheme in figure 3.

**Figure 4.** Dependence of vulnerability parrying time on the number of simultaneous attacks.

The graphs show the advantage of automatic determining the most optimal list of mechanisms for countering vulnerability by software emulation of the neural network compared to the standard system of switching services of the information system.

**Figure 5.** The dependence of the probability of defeat of electronic storage services on the number of simultaneous attacks.

In the framework of experimental studies developed by neural network implementations, the evaluation of the computation time as a function of the amount of initial data involved in combinatorial enumeration was carried out (table 1). As a time parameter, \( S(n) \) standard indicator is
used, which associates some abstract time of its calculation (problem solution) to each $n$ set of input data. The analysis showed a gain in the use of neural network by the criterion of suitability (time - accuracy) in solving reobring problems.

| $n$ / $S(n)$ | 20  | 50  | 100 | 200 | 500 | 1000 |
|--------------|-----|-----|-----|-----|-----|------|
| 1000n        | 0.02 s. | 0.05 s. | 0.1 s. | 0.2 s. | 0.5 s. | 1 s.  |
| 100n         | 0.04 s. | 0.25 s. | 1 s.   | 4 s.  | 25 s. | 2 min. |
| $HC$         | 1.7 s. | 4.1 min. | 22.1 min. | 56.1 min. | 1.3 h. | 2.8 h. |
| $n^5$        | 3.2 s. | 5.2 min. | 2.8 h. | 3.7 d. | 1 year | 31.7 y. |
| $2^n$        | 1 s.   | 35 years | $3*10^4$ y. | - | - | - |
| $3^n$        | 58 min. | $2*10^6$ y. | - | - | - | - |

5. Conclusion
The well-known algorithms [13–16], based on the dynamic programming method, the simplex method, the branch and bound method, and various heuristic approaches do not allow overcoming the “curse of dimension” that overlays the considered class of problems. The use of the class of dynamic neural networks and self-organizing maps to solve the problem of finding the most likely route of spreading the vulnerability of an information system is due to the display of a multidimensional distribution in the space of vulnerabilities of graph vertices with the corresponding attributes on a one-dimensional circle route. Kohonen's network allows ensuring that the condition that the most probable route of vulnerability satisfies must be met: close vulnerabilities in space should be mapped to close vulnerabilities in a one-dimensional route.

It should be noted that the proposed approach to the implementation of a system for protecting corporate information systems is not an alternative and does not contradict special requirements and recommendations about the technical protection of confidential information in state cultural institutions (museums, electronic libraries, etc.). The implementation of the methods within the framework of the approach optimizes the use of standard means of protecting software of large-scale electronic repositories, typical for large cultural institutions in time and effectiveness (reliability).

References
[1] Shrayberg Y 2018 Libraries in the conditions of the transforming book market Bibliography 5 3-10
[2] Bajpai M 2015 Researching through QR codes in libraries 4th International Symposium on Emerging Trends and Technologies in Libraries and Information Services (Noida) pp 291-4
[3] Gul S, Shafiq H, Nisa N, Hussain A, Shueb S and Shafi S 2018 World Digital Library World Cultures in One Click 5th International Symposium on Emerging Trends and Technologies in Libraries and Information Services (Noida) pp 54-8
[4] Wulandari L, Sularto L, Yusnitasari T and Ikasari D 2017 User Requirements Analysis For Digital Library Application Using Quality Function Deployment J. Phys.: Conf. Ser. 818 012004
[5] Merkl D and Rauber A 2000 Digital libraries-classification and visualization techniques International Conference on Digital Libraries: Research and Practice (Kyoto) 434-8
[6] Caihong G A 2016 study on strategies to improve the protection of personal information for university libraries users International Conference on Applied System Innovation (ICASI) pp 1-3
[7] Akinina N, Gusev S, Kolesenkow A and Taganov A 2017 Construction of basic graphic elements library for geoinformation ecological monitoring system 27th International Conference Radioelektronika (RADIOELEKTRONIKA) pp 1-5
[8] Dimitrienko Y and Gubareva E 2018 Neural network model of mathematical knowledge and
development of information and educational environment for mathematical training of engineers. J. Phys.: Conf. Ser. 1141 012010

[9] Krakovsky Y, Luzgin A and Ivanyo Y 2019 Cyberattack intensity forecasting on informatization objects of critical infrastructures IOP Conf. Ser.: Mater. Sci. Eng. 481 012003

[10] Golovko V 2001 Neural networks: training, organization and application (Moscow: IPRJR)

[11] Kaminski M and Bastrzyk A 2018 Modelling of oil agglomeration of dolomite by the use of an artificial neural network optimized using Optimal Brain Damage algorithm IOP Conf. Ser.: Mater. Sci. Eng. 427 012012

[12] Pratap U S, Tiwari A, Kumar R S and Dubey D 2017 Kohonen neural network model reference for nonlinear discrete time systems 3rd International Conference on Computational Intelligence & Communication Technology (CICT) pp 1-5

[13] Propoi A and Krivonozhko V 1978 The simplex method for dynamic linear programs (Laxenburg, Austria)

[14] Syahputra M F et al 2018 Genetic algorithm to solve the problems of lectures and practicums scheduling IOP Conf. Ser.: Mater. Sci. Eng. 308 012046

[15] Gafarov E, Lazarev A and Werner F 2010 Algorithms for some maximization scheduling problems on a single machine Automation and Remote Control 10 2070–84

[16] Lazarev A and Gafarov E 2011 Theory of scheduling: problems and algorithms (Moscow: Lomonosov Moscow State University)