Models and methods of information reliability and data protection

IOP Conf. Series: Materials Science and Engineering **537** (2019) 052001 doi:10.1088/1757-899X/537/5/052001

Models and methods of information reliability and data protection

G I Korshunov[12], V A Lipatnikov[3], V A Tichonov[3], A G Varjapetyan[1] and M S Smirnova[1]

[1]Saint-Petersburg State University of Airspace Instrumentation, 67A, Bolshaya Morskaya Str., Saint-Petersburg, 190000, Russia
[2]Peter the Great St. Petersburg Polytechnic University, 29, Polytechnicheskaya Str., Saint-Petersburg, 195251, Russia
[3]S. M. Budjonny Military Academy of the Signal Corps, Tikhoretskiy Prospekt, 3, Saint-Petersburg, 194064, Russia

E-mail: kgi@pantes.ru

Abstract. The models and methods for managing the cybersecurity infrastructure of an integrated organization with data protection are considered. The system structures built on their basis provide intrusion detection and analysis of the intruder's actions. High probability of data security is achieved using neural-fuzzy networks and cognitive modeling. Structured control algorithms include monitoring and highlighting features of digital streams with data transfer protocols, intrusion detection, implementation of data protection, taking into account the dynamics of intruder actions.

1. Introduction

Cybersecurity (CS) aims to organize the security of the cyber environment integrated organization (IO), using a variety of components and approaches to security. CS is based on information reliability and data protection. CS is provided by various classes of data protection according SIEM (Security Information and Event Management) [1]. The main tasks of SIEM systems are the processes of collecting large amounts of heterogeneous data on security events and detecting incidents and security threats as a result of their processing [2, 3].

A known method of managing the security of information networks (IN) based on a dedicated server with container virtualization. Issues of recognizing intrusions and predicting the state of IN protection of the IO infrastructure are not fully considered. Proactive protection tools must ensure the collection of necessary information, security analysis, monitoring of the network status, detection of attacks, prediction, countering their implementation, misleading the attacker [3].

At the same time, the task of clarifying the classification in recognition of intrusions in intellectual methods of managing the IO infrastructure design bureau remains relevant. In the study of proactive data protection, not enough attention is paid to the analysis of the dynamics of the offender actions, which include cyber-invasion (CI) scenarios. There is a contradiction between the effective new means of CC and the existing methods of protecting IN [4]. The article deals with the actual problem of the infrastructure protecting of IO from intruders' violators. Improving information reliability and data

protection are achieved by reducing the time analysis of the dynamics of offender actions based on neuro-fuzzy networks and cognitive modeling.

2. Intrusion Detection

Figure 1 shows the control circuit of CS with an implemented two-level intelligent automated intrusion detection system (AIDS). The lower level of control is carried out by data collection and management agents included in the IN, implementing a constant analysis of the state of CS and the corresponding effects with its changes. The upper level of management provides support for decisions, providing the most complete information about the current state of the CS and possible states.

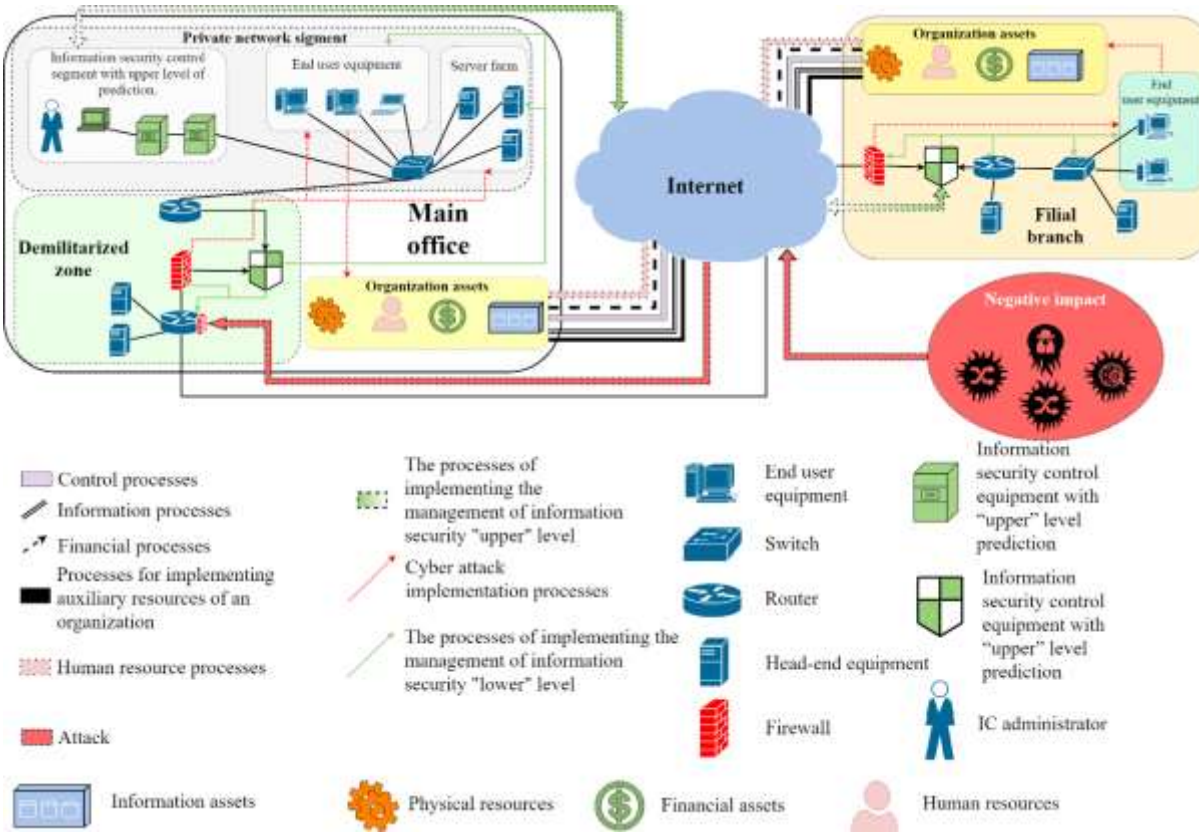

Figure 1. Infrastructure model of an integrated organization with the implementation of the proposed method of information reliability and data protection.

Figure 2 shows the block diagram of the implementation of the control method of the CS using the AIDS. The data collection process is carried out by obtaining information (“0”) from telecommunications equipment and information security tools using service information exchange protocols (SNMP, Syslog, IPMP, etc.), which is subsequently unified, filtered, and prioritized for further processing., The processed information from the output of the data collection module ("1")is fed to the input of the modules "Assessment of the state of protection", "Vulnerability forecast module" and "forecasting CI", these processes run parallel to each other.

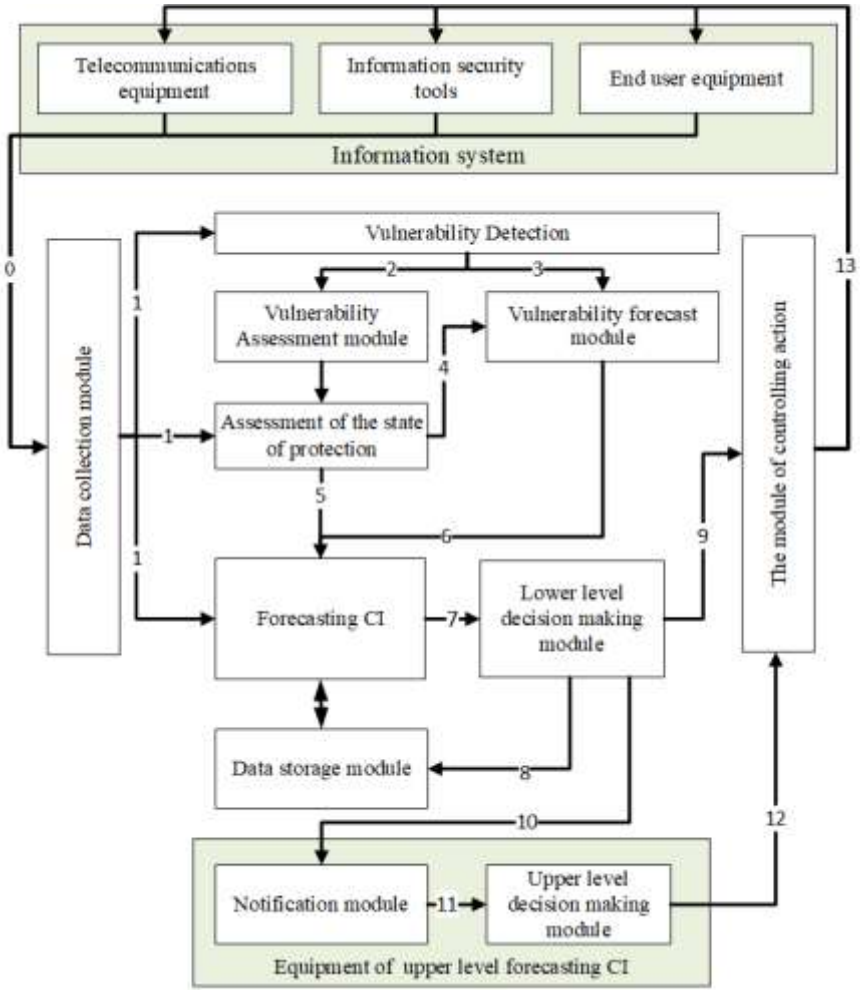

Figure 2. Structural diagram of the implementation of the control method of CS using distributed intelligent AIDS.

The module for detecting vulnerabilities is implemented through the use of previously known approaches, for example, in [5]. Information on detected vulnerabilities from the output of this module ("2") is fed to the input of the "Vulnerability Assessment module", which determines the degree of threat from the resulting vulnerability in accordance with the risk-based approach, as well as to the input of the "Vulnerability forecast module" ("3").

The module for assessing the state of protection [7, 8, 9] determines the indicator of protection based on information obtained from the modules implementing the "Vulnerability Assessment", "Forecasting CI" processes and information from the output of the data collection process ("1"). The complex indicator goes to the inputs of the "Vulnerability forecast module" and "Forecasting CI" processes ("4" and "5", respectively), this indicator allows to increase the quality and accuracy of the forecasts made.

Information from the modules implementing the processes: "Data collection module", "Assessment of the state of protection", "Vulnerability forecast module" and the "Data storage module" receives to the input of the block implementing the "Forecasting CI" process. Information from the data acquisition unit contains the general state of the system at the moment: the state and processes occurring in telecommunications equipment and information security tools. Information about the state of security of the information system ("5") allows evaluating data from the equipment ("1"), taking into account the complex security indicator and, together with information about forecasted vulnerabilities ("6"), displays the most complete information system status in terms of information security. The CC prediction process is carried out using the previously accumulated information from the data storage module, in order to improve the quality and accuracy of the forecast. The result of forecasting ("7") enters the "Lower Level Decision Making module", the result of which is the determination of the degree

of competence of the automated lower level control processes - the level of measures implemented within the same branch and not significantly affecting the CS and the IN as a whole. If it is necessary to apply CS control that exceed the lower level, the information is communicated to the decision maker (IC administrator) ("10" and "11") whose activities are decisions ("12") aimed at shaping compensating impacts ("13") on the information system prevent the occurrence of intrusions. In other cases, the result of decision making is fed to the block of formation of compensating influences to prevent intrusions. The data storage module contains information about previously implemented forecasts and compensating impacts.

3. Analysis of the dynamics of the offender actions

The incoming heterogeneous information is prepared for subsequent analysis and processing at the planning stage, this stage is represented by a set of "Primary data processing" blocks in figure 3. The implementation phase is carried out by a modular hybrid time series forecasting system. This system is designed to predict the time series, showing with a certain probability and forecasting horizon the possibility of the occurrence of CS. The test consists in the constant assessment of the forecast carried out by the criteria of accuracy, relevance and compliance with the forecast horizon. The improvement was implemented due to the correction module, which provides a corrective effect on neural networks and cognitive maps of the Data Analysis Block. The full block diagram of the implementation module of the prediction process of CS is presented in figure 3, the data analysis module is presented in figure 4.

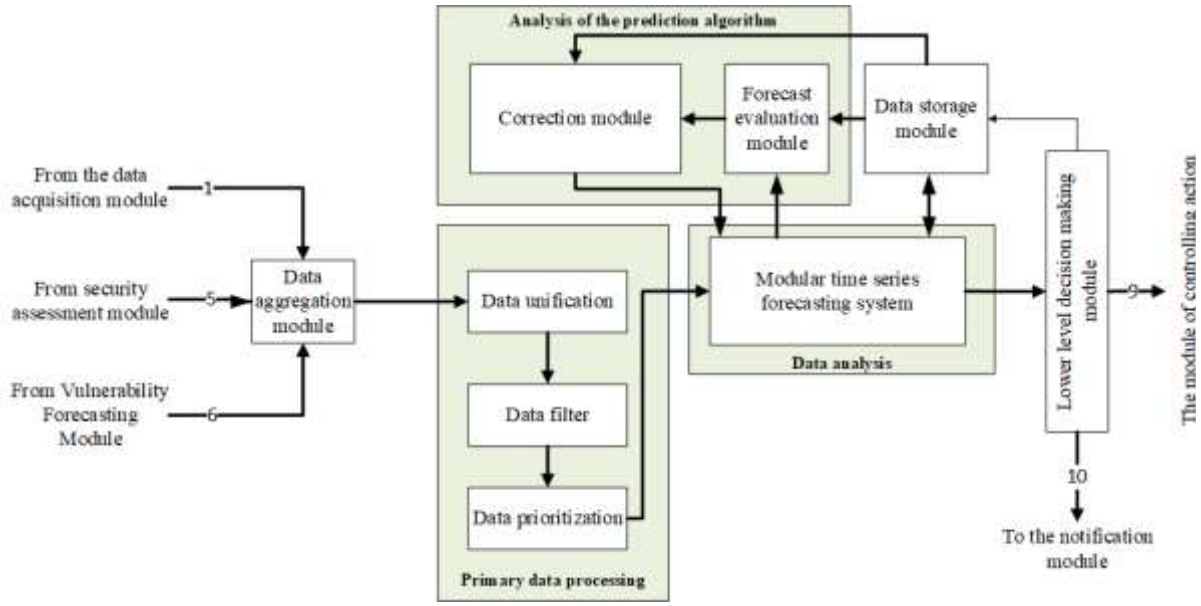

Figure 3. Block diagram of the prediction model of cyber intrusion.

A modular hybrid time series prediction system was chosen for data analysis, similar to that described in [6]. Due to modularity [11,12,13], the system has additional fault tolerance - when failures of composite modules fail, the rest continue to perform their work. The block diagram of the module is presented in figure 4.

This system is based on three main modules that carry out the task of forecasting: a neuro-fuzzy network, a fuzzy cognitive map and a neural network (NN), analyzing the dynamics of the offender actions and the final forecast., there is a parallel processing of the incoming information in this system, which increases both quantitative and qualitative characteristics, and the results of the work of these blocks go through a verification stage confirming the adequacy of the forecast [14]. The terminal unit, implemented by the neuro-fuzzy network, provides the resulting forecast, which enters the external

processes of the lower level decision making module ("7"), the data storage module and the module of the state of IS security, and the internal forecast evaluation process.

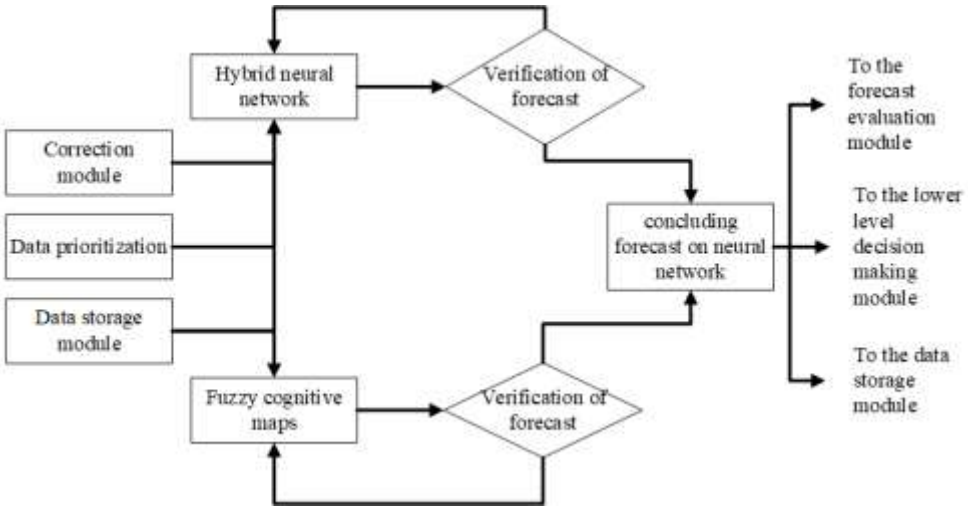

Figure 4. Block diagram of a modular time series forecasting system.

Conclusions

The developed block diagram of information systems with intrusion recognition agents and prediction of the state of the information security infrastructure of the information processing unit provides information reliability and data protection. The developed control algorithms for detection and recognition of intrusions are used to support decision-making during intellectual protection processes, taking into account the dynamics of the intruder actions. Solving the problem is achieved by integrating such data mining methods as a neuro-fuzzy network to solve specific problems of classification and algorithms for making decisions on responding to security incidents into the general process of monitoring IS. Based on the approach used in [10] to assess the security of an IO, the dependence of the probability of protection on time is constructed - figure 5. A significant gain in the probability of being protected by the proposed approach P2 (t) as compared to the methods implementing reactive control methods P1 (t) was obtained taking into account the cyclical nature of the process of information protection under control of the CS.

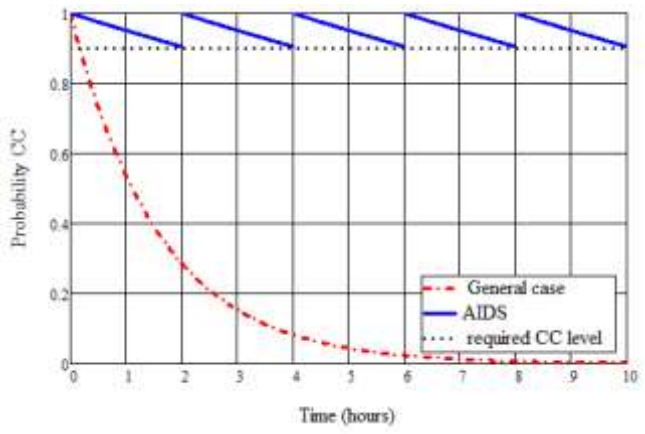

Figure 5. Graph of the probability of protection of the IO as the function of time.

The proposed approach makes it possible to ensure the CS of the protected infrastructure of the IO based on the use of the event prediction model. The presented structures implement the CS management method based on intelligent adaptive data protection services. Information about security events is generated at the infrastructure level, subject to preprocessing at the data level, distributed to the required elements of the application layer and, ultimately, finally processed by the elements of this last level.

References

[1] Andrianov V, Krasov A and Lipatnikov V 2012 *Innovative Information Security Risk Management* (St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications) p 396
[2] Lipatnikov V, Shevchenko A and Yackin A 2017 Information Security Management of Integrated Structure Organization based on a Dedicated Server with Container Virtualization *Information and Control Systems* **4(102)** 116-26
[3] Kuznecov I, Lipatnikov V and Shevchenko A 2016 Multivariable control technique of information telecommunication network security of integrated structure organization quality management system *Questions of radio electronics* **6** 23-8
[4] Korshunov G, Lipatnikov V and Shevchenko A 23-25 October 2018 Decision support systems for information protection in themanagement of the information network *Fuzzy Technologies in the Industry FTI 2018* (Russia Ulyanovsk) pp 418-26
[5] Karganov V, Kostarev S, Lipatnikov V, Lobashev A and Shevchenko A 09.11.2017 The way to protect a computer network from unauthorized impacts *Patent 2635256* **(**Russian Federation)
[6] Yarushev S, Averkin A and Fedotova A 2017 Modular model for time series forecasting based on neuro-fuzzy nets and cognitive modelling *Fuzzy Systems and Soft Computing* **12(2)** 159–68
[7] Camacho E and Bordons C 2004 Model predictive control (London: *Sprinder Verlag)* p 405
[8] Batina I 2004 Model predictive control for stochastic systems by randomized algorithms (Eindhoven: Technische Universitaet Eindhoven)
[9] Byres E and Lowe J 2003 The myths and facts behind cyber security risk for industrial control systems *ISA Process Control Conf.*
[10] Korshunov G, Lipatnikov V, Shevchenko A and Malyshev V 2018 Adaptive Management of Information Network Protection with Analysis of Intruder's Actions *Information and Control Systems* **4** 61-72
[11] Sheth H, Shah B and Yagnik S 2014 A survey on RBF Neural Network for Intrusion Detection System. *Int. Journal of Engineering Research and Appl*. **4** 17–22
[12] Ryan J and Lin M 1998 Intrusion Detection with Neural Networks *Advances in Neural Information Processing Systems* pp 943–9
[13] Tan K 1995 The Application of Neural Networks to UNIX Computer Security *Proc. of the IEEE International Conf. on Neural Networks* **1** 476–81
[14] Lukatskii A Attack detection 2008 (St. Petersburg: BHV- St. Petersburg) p 304