IT security in special purpose networks

N.V. Kireeva¹, T.V. Filippova¹, O.A. Karaulova¹ and M.V. Aleshin²

¹Volga State University of Telecommunications and Informatics Samara, Samara, Russian Federation, zeppelinsn@yandex.ru
²National Technology Initiative Center for Advanced Manufacturing Technologies based on the Institute of Advanced Manufacturing Technologies of Peter the Great St. Petersburg Polytechnic University Polyteknicheskaya, 29, St.Petersburg, 195251, Russia

Abstract. The article highlights the problem of ensuring secure communications in special purpose networks, in particular, the insufficient status of domestic telecommunication services market development. To ensure secure communication the measures must be sufficient for the strict functionality and information security requirements and they must have the respective certificates. Certificating is a time taking process and the issue of using foreign made items remains the issue of the day. The article covers burning issues of cyberattack countermeasures, the ways of solving IT security issues on essential IT segments of a special purpose network.

Keywords: cyber security/ IT security, dedicated network, essential IT segments, cyberattack countermeasures

1. Introduction

The most important component of information security technology is the cyberattack countermeasures on essential IT segments. Essential IT segments are those subsystems and research institute objects, which breach of database causes significant damage to the economics, national security and national interests of the country.

1.1 Secure communications ensuring in special purpose networks

Dedicated networks are needed for government authorities, the national defense demands, national security and enforcement of law and order. The need of integration of various types of services, such as telephone, fax communications, video communication, data transfer, has led to the plain old telephone service and the multiservice communication networks development. Traditional public telecommunications are built on the basis of TDM technology (Time Division Multiplexing) [1]. At the present stage of the telecommunications development digital TDM-PBX (Private branch exchange) is losing its market dominance due to the possibility of providing a wide range of services from systems based on packet switching mode while data transferring [2].

IP packet switching is implemented in the so-called Next Generation Networks (NGN), which are designed to provide telecommunication services and to use several wideband transport technologies with QoS on. The basis of NGN networks, originally NGN IPCC (International Packet Communication Consortium), are flexible switches such as Soft switch and IP-ATS. NGN is an upgraded TDM network with the ability to transmit IP traffic, as well as with additional capabilities to provide services to the end user.

Currently TISPAN is replacing the IPCC in NGN, which key element is IMS (IP Multimedia Subsystem). The main difference between NGN TISPAN (IMS) and NGN IPCC is the flexibility and
scalability of such networks. Here the session control and routing control functions are performed by the CSCF (Call Session Control Function), which replaced the Soft switch. On the one hand, NGN IPCC / TISPAN (IMS) networks provide a wide range of additional services (so-called VAS – value added services) that provide more efficient network management capabilities comparing to the TDM architecture. On the other hand, this range of functionality increases the number of insecurities and gives rise to sources of information security threats (Fig. 1).

Figure 1. NGN project implementation

Taking into account the nature of the information transferred through the dedicated network, the issue of using secure patching facilities is especially relevant [4]. In order for the means of communication to be used in dedicated network it must meet the requirements of the Federal Security Service of Russia (FSB), FSTEC (Federal Service for Technology and Export Control) or the Ministry of Defense of Russia and must have the appropriate certificates. The security requirements for ATS and ATS control systems has a number of restrictions on advanced features of equipment, hacking protection requirements and signaling if it occurs, event registration (logging), access control and management. Consequently, the certification of IP ATS, including those currently available on the market, is quite a challenge taking into account the above mentioned security requirements.

The issue of ensuring secure communication in special-purpose networks today is the issue of the day, it requires the development of telecommunication market (especially the domestic communications industry development), which must meet strict requirements of functionality and information security.

1.2 Cyberattack countermeasures in special purpose networks.

The main tasks of essential IT segments are: — master data transmit and receive for computational analysis; — logging, data storage and delivery of information at control point; — delivery, logging and management data delivery to control centers subscribers; — information exchange between subscribers of points and control centers; — organization of operational interaction and management between essential IT segments through communication channels. The topology, structure and functions of essential IT segments are formed on the basis of unified information and telecommunication facilities in accordance with the requirements for controlled objects [3,4]. Methods and protocols of information interaction of essential IT segments subscribers for each specific control object are implemented by organizing communication with subscribers, combining measuring, logging, data processing and transmit. Each essential IT segment can have an optional switching mode, which considers the specificity of hardware and software.

Currently under conditions of cyberattacks, the effectiveness of essential IT segments as the main important and controlling component of automated systems is largely determined by the stability of essential IT segments of logging, processing and transmission of information [5,6]. With the old-fashioned computer facilities and computer systems replacement in essential IT segments, cyberattacks became possible in principle because of critical areas in digital communication equipment and using
software in remote access mode through transparent networks (both for a system operator and attacker) based on standard data transfer protocols. The consequence of cyberattacks can be the control information blocking and the false data introduction, violation of logging fixed regulations, processing and transmission of information in control complexes, failures of essential IT segments, as well as discrediting of information received by consumers [7].

The applicability of the proposal development, which will neutralize the cyberattacks and at the same time maintain the stability of essential IT segments during the management production run, is due to the following factors:

─ the intensive technologies development and cyberattacks implementation tools;
─ danger of loss of essential IT segments stability during cyberattacks;
─ the forced necessity to implement foreign-made hardware and software into essential IT segments;
─ the impossibility to stop the cyberattacks increase by traditional methods and information protection tools;
─ imperfection of cyberattacks countermeasures.

The development of cyberattacks countermeasures on essential IT segments is based on the multipurpose use of the information protection theory, the stability and reliability of automated systems, complex system modeling, automatic control, information quality and reliability, cyberattacks discovery.

Conclusion

The results of modern approaches analysis of information protection, ensuring the reliability and stability of essential IT segments functioning show that they have not fully solved the following issues:

─ issues related to the methods and models development for countering cyberattacks on the tools of logging, processing and transmitting information from essential IT segments, intelligent tools for monitoring the state of the information computation process and the organization of an active cyberattacks countermeasures have not been considered;
─ most of the known cyberattack detecting methods and models do not take into account the interconnected dealing with the cyberattacks countermeasures and the stability of essential IT segments during the management production run;
─ there are practically no complex methods, models and algorithms where along with signature attacks analysis and essential IT segments anomalies detection the detection of attacks is carried out by functional analysis of controlled parameters and identification of stability state of essential IT segments;
─ methods and models of decision making including statistical approach to ensure active cyberattack countermeasures are not well developed.

In addition, the currently used methods and models for countering cyberattacks on essential IT segments do not resolve a number of contradictions:

─ between increasing the efficiency and stability of the control system, on the one hand, and decreasing of management processes under the influence of computer attacks on essential IT segments, on the other hand;
─ between reducing the number of vulnerabilities factors of essential IT segments, requiring the elimination of extra functions and parameters, on the one hand, and complicating the information and computing monitoring process in essential IT segments and detecting attacks, on the other hand;
─ between the requirements for the timeliness of the control technology cycle, on the one hand, and the time required to detect and neutralize the source of the attack, on the other hand.

One of the possible ways to create cyberattack protected essential IT segments is the essential IT segments information technologies integration with cyberattack countermeasures sensors set up in its structure, in compliance with the mandatory interaction of administrative tools with cyberattack countermeasures control programs.

At the same time, essential IT segments security will be achieved when the complex use of organizational and technical measures, the maximum use of administrative and network monitoring tools, antivirus tools, certified software, computer and switching equipment are used along with cyberattack countermeasures components.
Besides, it is necessary to generate a list of extreme monitored parameters of essential IT segments, to determine their sensitivity to cyberattacks, to experimentally verify the consistency of essential IT segments components, cyberattack countermeasures, means of protecting information from unauthorized access when performing real technological cycles of cyberattack control, and to develop (specify) technical solutions based on changes in the controlled parameters. This will help us to solve the issue of information security ensuring and information protection on essential segments of the special-purpose network.

We can distinguish two contradictory approaches to ensuring information security. Russia like China sticks to the position of the need of total informational space demilitarization. According to the Russian Federation the arms race in the informational space can disrupt existing agreements on disarmament and international security.

The United States like the EU maintains the position that the main threats to cybersecurity are cyberterrorism and cybercrime, and the issues of interstate confrontation in cyber space should be regulated within the international humanitarian law.

References

[1]. Druk E.V. Fundamentals of organization and management of VPN-networks of modern information systems for special purposes // T-Comm: Telecommunications and transport. 2019.Vol. 13.No. 6.P. 19. (In Russian)

[2]. Goldstein B.S. Communication networks: Textbook for universities. SPb.: BHV Saint Petersburg, 2018.S. 29. (In Russian)

[3]. V.V. Karganov To prevent and ensure the required level of information security of a special-purpose information-computing network from unauthorized impact // Questions of defense technology. Series 16: Technical means of countering terrorism. 2018.No. 2.P. 78. (In Russian)

[4]. Baklanov I.G. NGN: principles of construction and organization. M.: Eco-Trends, 2017.S. 28 (In Russian)

[5]. Zegzhda, D. P., Lavrova, D. S., & Pavlenko, E. Y. (2020). Management of a dynamic infrastructure of complex systems under conditions of directed cyber attacks. Journal of Computer and Systems Sciences International, 59(3), 358-370. doi:10.1134/S1064230720020124

[6]. Zegzhda, D. P., & Stepanova, T. V. (2015). Approach to APCS protection from cyber threats. Automatic Control and Computer Sciences, 49(8), 659-664. doi:10.3103/S0146411615080179

[7]. Zegzhda, P. D., Zegzhda, D. P., & Stepanova, T. V. (2015). Approach to the construction of the generalized functional-semantic cyber security model. Automatic Control and Computer Sciences, 49(8), 627-633. doi:10.3103/S0146411615080192