Kultura Bezpieczeństwa
Nr 38, 2020 (57–65)
ISSN 2299-4033 DOI: 10.5604/01.3001.0014.5939

MEASURES FOR PROTECTION OF THE INFORMATION SYSTEMS OF UKRAINE'S CRITICAL INFRASTRUCTURES AGAINST CYBERATTACKS

Yurii Kohut*

ABSTRACT
The article deals with protective measures against cyberattacks of information systems of the critical infrastructures and highlights some features of the cyberattacks against the information resources of national authorities. The main objective of the article is to define the characteristics of cyberattacks and the elements of a plan to counter cyberattacks of the critical information facilities. It has been found that a professionally organized cyberattack consists of several phases related to targeting, intelligence, access to the system, direct execution of the attack, and destruction of evidence of unauthorized interference. The results show that to protect the critical infrastructure facilities from cyberattacks, developed and implemented national cybersecurity standards must be developed in Ukraine, in particular for automated control systems of critical infrastructure facilities.

KEYWORDS
cyberattack, information system, critical infrastructure, cybersecurity

* Yurii Kohut, M.A., Interregional Academy of Personnel Management, Ukraine, Kyiv; email: office@sidcon.com.ua

INTRODUCTION

The globalization of connectivity creates major vulnerabilities to key critical national information infrastructures.[1] The protection of the critical military, political, social and economic infrastructure of states from cyberattacks is gradually becoming one of the highest priorities in ensuring national security. When the high level of cyberterrorism threats is combined with the rapidly increasing level of reliance on information technology by society, the issue is particularly relevant and requires a coordinated and comprehensive national response.

Many critical infrastructures, such as electricity, water supply, transport, etc., are operated in states, including Ukraine, by means of computer-based dispatch and data collection systems. These systems may be attacked with the aim to disrupt their functioning and eventually cause physical damage and destruction, such as the discharge of water from the dam, the transfer of railway tracks and the subsequent collision of trains, or the violation of air traffic control services and aircraft accidents.

Recent cyberattacks using malware such as Stuxnet, Duqu, Flame, or Gauss have shown how vulnerable IT infrastructure of fuel and energy, production, transport and information technology, community, financial and other life support systems are, and how disastrous the consequences of such cyberattacks and the failures of these systems can be.

Cyberattacks against the information resources of national authorities are also common. For example, the number of reported cyberattacks on servers and networks serving United States federal authorities, according to the U.S. Department of Homeland Security (Computer Emergency Readiness Team, US-CERT), as of 2010, totalled more than 41,000 cases.[2]

As the experts point out, it is sufficient to launch an effective cyberattack on several dozen critical objects in Central Europe in order to stop the normal functioning of one or more states; in this respect, the disabling of nuclear power plants and hydraulic facilities would have the most lasting negative consequences.

[1] V. Auzan, D. Afrin, *Tehnologii protiv setey*, “Expert”, 15 October 2001, no. 38, pp. 37–38.

[2] *US Computer Emergency Readiness Team*, http://www.us-cert.gov (accessed: 17.10.2020).

METHODS

The methodological basis of the study is formed by the general scientific principles of the systemic approach; by the analytical methods (logical, factual, comparative, strategic, managerial); and by the quantitative and qualitative research into the main trends of the formation and development of critical infrastructure, sectoral management, etc.

FINDINGS AND DISCUSSION

Cyberattacks on public critical infrastructure information systems fall into two huge categories:[3]

- cyberattacks disabling information systems: hacker attacks of this type are the most common, aimed at temporarily disabling individual control systems or distorting program information. The result of such actions is the uncontrolled functioning of the targeted object, which is particularly dangerous in case of nuclear and chemical production, as well as in the military sphere – electronic protection systems and attacks;
- destructive attacks: cyber-terrorist operations against information system facilities may result in the destruction of information resources and communication lines or in the physical destruction of information system entities. If systems are involved in critical infrastructures, in the worst-case scenario, network cyberattacks can have as wide-ranging consequences as traditional bombings.

Cyberthreats to critical infrastructure have the following characteristics:[4]

- critical infrastructure risks encompass the responsibilities of different agencies;
- information critical infrastructure is highly vulnerable;
- the protection of critical information infrastructure facilities should be ensured at all sites, regardless of the form of ownership.

Experts identify the following groups of cyberattacks against critical infrastructure:

[3] V.A. Mazurov, *Kiberterrorizm: ponyatie, problemi protivodeystviya*, "Doklady TUSURa" 2010, vol. 1(21), no. 1, p. 43.

[4] D.S. Biriukov, *Do pytannia pro zakhyst krytychnoi infrastruktury vid kiberatak*, [in:] *Protydiia teroryzmu, nerozpovsiudzhennia zbroi ta materialiv masovoho znyshchennia y zakhyst krytychnoi infrastruktury (zbirnyk materialiv zasidan Mizhvidomchoi ekspertnoi robochoi hrupy, stvorenoi pry Natsionalnomu instytuti stratehichnykh doslidzhen)*, O.D. Markeeva (ed.), Kiev 2013, pp. 65–76.

- attacks on servers and networks serving authorities, financial institutions, large companies;
- attacks on Automated Control Systems (ACS) of industrial facilities.

The latter group of attacks is attracting increased attention, as unauthorized interference with automated control systems of production process (ACS PP) of critical infrastructure facilities can have dire consequences.

Previously, experts had considered that ACS PP were well protected from external unauthorized interference, as they were generally isolated from external computer networks and used specific hardware and software. But after the discovery of the first occurrence of ACS PP infection of industrial facilities in Iran with the virus Stuxnet in 2010, the vulnerability degree of these systems was no longer underrated. As a rule, such cyberattacks are accompanied by preliminary collection of confidential information about the object of a possible attack with the help of virus-spies such as Duqu or Flame. This is confirmed by the information released in March 2012 on the detected attempts to interfere with the work of ACS PP of gas transportation system facilities in the USA.[5] An investigation into the effects of the attempted interventions revealed that the cyberattacks belonged to the same group and were linked to phishing activities directed against the gas transport operators since December 2011.

As one analyzes publications in the field of information security of critical infrastructure management systems, one should notice the following:

- Modern software, combined with publicly available information, enables even less experienced attackers to cyberattack systems and hardware of infrastructure networks such as high-voltage power lines.[6]
- The number of identified vulnerabilities is growing rapidly. In the first three quarters of 2013, more vulnerabilities in critical infrastructure ACS PP were published in specialized databases and manufacturers' reports. Since 2005, more vulnerabilities in critical infrastructure ACS PP have been reported.[7]

[5] *Ibidem*.

[6] *Increasing Threats to Industrial Control Systems. ICS-CERT Alert 12-046-01A*, "US-CERT", 25 October 2012, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-046-01A.pdf (accessed: 3.11.2020).

[7] G. Grytsay, A. Timorin, Yu. Goltsev, R. Iliin, S. Gordeychik, A. Karpin, *Bezopasnost promyishlennyih sistem v tsifrah*, Moskva 2012, http://filearchive.cnews.ru/doc/2012/06/scada.pdf (accessed: 5.11.2020).

- Vulnerabilities are primarily found in the most common equipment models; one in five vulnerabilities have not been closed within a month; about 65% of vulnerabilities are of high and critical risk; every second vulnerability gives the attacker the ability to execute arbitrary commands on an ACS PP-attacked of critical infrastructure.[8]
- The USA and the EU countries are leading in the number of governance systems that can be accessed via the Internet, and they remain the most vulnerable to this threat, in particular because of disregard for information security (errors in system configuration, weak or standard passwords, etc.).[9]

The potentially vulnerable elements of the enterprise's information infrastructure that are most commonly used as targets for cyberattacks on ACS PP of critical infrastructure can be identified as:

- an enterprise server having the way out to the "outside world" (it is subjected to constant cyberattacks via the Internet);
- home mobile computers (laptops, tablets, smartphones, etc.) which operate on the basis of a common operating system (OS), have vulnerabilities and are used by employees and management to share data with company (secure) computers (data is sometimes transmitted between a home computer and a company computer);
- hardware (computers) with local network connection;
- computers that have ports to connect removable drives, disk drives to read information from optical disks.

Coordinated cyberattacks using software viruses pose a significant threat to critical infrastructure security. This type of attack consists of the preparatory phase (actions that create new vulnerabilities on the object) and the attacking actions (exploiting existing vulnerabilities).

The main countermeasures used to manage the cybersecurity of the ACS PP of critical infrastructure facilities are:[10]

[8] I.N. Fovino, A. Carcano, M. Masera, A. Trombetta, *An experimental investigation of malware attacks on SCADA systems*, "International Journal of Critical Infrastructure Protection" 2009, vol. 2, issue 4, pp. 139–145, DOI: 10.1016/j.ijcip.2009.10.001.

[9] E. Luiijf, *Assessing and improving SCADA security in the Dutch drinking water sector*, "International Journal of Critical Infrastructure Protection" 2011, vol. 4, issues 3–4, pp. 124–134, DOI: 10.1007/978-3-642-03552-4_17.

[10] US Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, October 2009.

- implementation of a security policy (security policy should be developed for the management network and its individual components; it should be reviewed periodically to take into account new threats and system functionalities);
- control of access to resources and services;
- detection of malicious activity (usually in the form of regular monitoring of log files by experienced administrators and the usage of intrusion detection systems);
- mitigation of possible cyberattacks (control by administrators of access to vulnerability in such a way that vulnerability cannot be exploited in cases where the elimination of vulnerability may lead to system failure or inefficiency);
- fixing bugs in the system core which always requires updating of the software (network, operating system, or application software).

A professionally organized cyberattack consists of several phases related to targeting, intelligence, access to the system, direct execution of the attack, and the destruction of the evidence of unauthorized interference. Therefore, an overall plan to counter cyberattacks on critical information infrastructure should involve such activities:

- enabling timely detection and response to cyberattacks;
- monitoring and addressing identified vulnerabilities;
- repair of damaged systems, networks and equipment;
- reducing (minimizing) the impact of such cyberattacks.

The author believes that in order to prevent the failure of information systems and automated control systems of critical infrastructure facilities in Ukraine, priority measures for the protection of such facilities are as follows:

1. Development of a national program to secure critical information infrastructures.
2. Establishment of nationwide and regional information security management and cyber-terrorism systems (in other words, systems for detecting, preventing and responding to cyberattacks on critical information infrastructure). A nationwide coordinating authority could become a key part of Ukraine’s system for managing information security and countering cyberterrorism. It might be a service or department that already exists, such as the State Service for Special Communications and Protection of Information of Ukraine, or a newly created one, such as the National Centre for Countering Cyberthreats. It could assume the

functions of gathering and analysing data on the level of information security of critical segments of the state's information and telecommunications infrastructure. On the basis of its data, organizational decisions could be taken to ensure the necessary level of security of the information and telecommunications infrastructure of Ukraine.

3. Development of security policy of the IT infrastructure of critical important facilities (CIF). In particular, the security of the CIF IT infrastructure should be assessed from the point of view of the reliability of those nodes that, if accessed by the attacker, are most likely to cause harm.
4. Establishment of a state-level register of key information infrastructure systems in Ukraine, identifying the risk of cyberattacks on these facilities.
5. Implementation of foreign best practices in information security and anti-cyber-terrorism measures. In particular, it is advisable for Ukraine to learn from the experience of its neighbour country, the Russian Federation, when it comes to the **implementation** of the following (restricted access) **guidelines**: *Basic information security threat model in key information infrastructure systems, General requirements for information security in key information infrastructure systems, Recommendations for information security in key information infrastructure systems, Methodology for identifying current information threats in key information infrastructure systems, System of features of critical facilities and criteria for assigning functioning information-telecommunication systems in their composition to the protection from destructive information influences.*
6. Inventory and vulnerability analysis of automated control systems of production process operating in Ukraine at high-risk infrastructure, strategic infrastructure, and other critical infrastructure.
7. Improved, developed and implemented national cybersecurity standards, in particular for automated control systems operating in critical infrastructure facilities.

CONCLUSIONS

The high vulnerability of the national information infrastructure allows unfriendly states, terrorist organizations, criminal groups and individual perpetrators to inflict damage on a country comparable to that of weapons of mass destruction. The author would like to emphasize the following: to deny today the existence of cyberterrorism in its various manifestations as a serious threat that challenges the international community is reckless and short-sighted. States, including Ukraine, face the challenge not only of clearly identifying the problem but also of developing effective legal and technical methods.

REFERENCES

Auzan V., Afrin D., *Tehnologii protiv setey*, “Expert”, 15 October 2001, no. 38, pp. 37–38.

Biriukov D.S., *Do pytannia pro zakhyst krytychnoi infrastruktury vid kiberatak*, [in:] *Protydiia teroryzmu, nerozpovsiudzhennia zbroi ta materialiv masovoho znyshchennia y zakhyst krytychnoi infrastruktury (zbirnyk materialiv zasidan Mizhvidomchoi ekspertnoi robochoi hrupy, stvorenoi pry Natsionalnomu instytuti stratehichnykh doslidzhen)*, O.D. Markeeva (ed.), Kiev 2013, pp. 65–76.

Fovino I.N., Carcano A., Masera M., Trombetta A., *An experimental investigation of malware attacks on SCADA systems*, “International Journal of Critical Infrastructure Protection” 2009, vol. 2, issue 4, pp. 139–145, DOI: 10.1016/j.ijcip.2009.10.001.

Grytsay G., Timorin A., Goltsev Yu., Iliin R., Gordeychik S., Karpin A., *Bezopasnost promyishlennyih sistem v tsifrah*, Moskva 2012, http://filearchive.cnews.ru/doc/2012/06/scada.pdf (accessed: 3.11.2020).

Increasing Threats to Industrial Control Systems. ICS-CERT Alert 12-046-01A, “US-CERT”, 25 October 2012, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-046-01A.pdf (accessed: 5.11.2020).

Luiijf E., *Assessing and improving SCADA security in the Dutch drinking water sector*, “International Journal of Critical Infrastructure Protection” 2011, vol. 4, issues 3–4, pp. 124–134, DOI: 10.1007/978-3-642-03552-4_17.

Mazurov V.A., *Kiberterrorizm: ponyatie, problemi protivodeystviya*, “Doklady TUSURa”, 2010, vol. 1(21), no. 1, pp. 41–45.

US Computer Emergency Readiness Team, http://www.us-cert.gov (accessed: 17.10.2020).

US Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, October 2009, https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf (accessed: 24.10.2020).

CITE THIS ARTICLE AS:

Y. Kohut, *Measures for protection of the information systems of Ukraine's critical infrastructures against cyberattacks*, „Kultura Bezpieczeństwa" 2020, nr 38, s. 57–65, DOI: 10.5604/01.3001.0014.5939.