DOI 10.15622/sp.2019.18.6.1333-1356

G.R. TSOCHEV, R.D. YOSHINOV, O.P. ILIEV

KEY PROBLEMS OF THE CRITICAL INFORMATION INFRASTRUCTURE THROUGH SCADA SYSTEMS RESEARCH

Tsochev G.R., Yoshinov R.D., Iliev O.P. **Key Problems of the Critical Information Infrastructure through SCADA Systems Research.**

Abstract. In the current age, cyber security is an essential element of any information system. A key aspect is in the critical information infrastructure, where information security has become a top priority for information and network security experts. The interoperability of an ICT infrastructure with other components of it is an important aspect of its life cycle. Because Supervisory Control and Data Acquisition (SCADA) systems form part of the critical infrastructure, their cyber protection is particularly important in strategically important industrial and infrastructure sites — power plants, refineries, oil pipelines, treatment plants, manufacturing facilities, communications and transportation infrastructures. Along with the advancement of technology, the increasing number of Scada devices available online, the vulnerability of the sectors controlled by them has also increased. In the world of Internet of things (everything), the end devices cause a new wave of possible vulnerabilities in SCADA. They become the new places for attacks and breaches trough wich the system may be accessed or even compromised. There are a number of critical infrastructures in the Community whose disruption or destruction would have significant cross-border implications for more than one sector as a result of the interdependence of interconnected infrastructures. Such European critical infrastructures have been established and launched under a common procedure developed by the European Commission, with security requirements assessed according to a common minimum approach.

The present article exposes and examines the critical infrastructures of the European Union and Bulgaria. Trough presenting the structure of a Scada system the vulnerabilities and the various possibilities of attacking it were analised. As an example, a specific case based on trees has been considered, and the obtained results were summarized and visualized. The consequences were analized and respecctive conclusion was done.

Keywords: Critical Infrastructure, SCADA, Attack Tree, Cyber Security, Network and Information Security.

1. Introduction. The last decade was filled with great dynamics in the field of information technology. Increasingly, terms such as cyber attacks, espionage, stolen personal information from hacked profiles in social networks or elsewhere have become more common.

In times of high technological growth and multiple directions of development, everyone is looking for their own way to succeed. Both the innovativeness and knowledge of the factors that lead to the successful implementation of the steps for implementing the final decision are decisive. For the most part, the information is contained in the shared network space. Its value is greater than ever, and may be increased or decreased by some of the characteristics it possesses [1]:

– availability allows authorized users — physical persons or computer systems – to access information without hindrance;

– information accuracy exists when it is free of errors and inaccuracies, and has the value that end users expect to have. If the information has been intentionally or inadvertently modified, it is no longer reliable and accurate;

– of major importance is the authenticity of information, and its quality and condition to be original. It can be considered authentic when it is on the same level at which it was created, stored or transmitted;

– information is confidential when it is protected from the disclosure or exposure of unauthorized users or systems.

For most organizations, the security of information and the systems that process, transmit, and store it is crucial. In many more cases, information is also business.

Creating an information security program that adheres to the principles of security as a business factor is the first step in an association's efforts in building an effective security strategy. Continuous risk assessment is necessary, as well as evaluating and implementing sound policies, standards, and controls in order to reduce them.

Computer systems and networks are one of the highest technological products of humanity. Apart from all the advantages they offer, they have a number of disadvantages. Security problems in the form of malware, loss of privacy, reception of unwanted advertising, commercial or spam messages affect almost every computer user. One of the many definitions of security is that it represents the ability of a system to withstand external or internal destabilizing factors that can lead to its undesirable state or behavior.

The purpose of information security is to protect the valuable resources (information, computer hardware and software) of an organization. By selecting and implementing appropriate safeguards, security assists the mission of the organization by protecting its physical and financial resources, reputation, legal position, employees and other tangible and intangible assets.

The endless development of technology has undoubtedly improved the efficiency of industrial processes, and the delivery of health services. Jobs that would take more time and work force have already been taken up by devices that are connected to each other to achieve the same goal and even make it better. Healthcare people now rely on information systems, including mobile devices (implantable or external), to facilitate patient monitoring, so delivery of services has become more automated [7]. These connected devices, called the Internet of Things, have grown significantly when it comes to meaning, number and value over the years.

Despite the enormous advantages of these systems, it is likely that these devices can be used by malicious cyber attackers as a means of endangering the system itself, and human existence in general. A highly motivated person or group of people for cyber-terrorism will endanger human lives and property by disrupting services provided by critical infrastructures, e.g. healthcare IT infrastructure. By endangering human life, the goals might be panic, personal injury, health risk or death. The satisfaction for the people

comes from the use of connected computer infrastructure to cause some physical impact on the environment.

Although various cyber attacks are already targeting IoT health services, pumps that overflow drugs are known to be very reliable and useful for doctors and patients as they provide safe and accurate administration of drugs and fluids. It is suggested that the attacker's motive should change from financial gain to altering the overflow rate of the overflow pump, changing the configuration of the device, sending malicious commands, or simply interfering with the communication of the device. The attacker may also decide to gain physical or remote access to the electronic health records (HER), and to modify the patient's files, such as blood type, type of dosage, therapy session, etc. All this can lead to catastrophic events and can also cause panic in society, especially if the event is unexpected — or there are no appropriate control measures in place.

An alternative industry relevant to this comparative study is the one that drives the industrial SCADA system [3]. No rigorous security research has been done when SCADA systems were introduced decades ago. This has led to many of the security problems that they face today.

2. Critical Infrastructure. The term **c**ritical infrastructure refers to an element, system or parts thereof located in Member States which is essential for the maintenance of vital public functions, health, safety, security, economic or social well-being of the population, and whose disruption or destruction would have significant consequences in a given Member State as a result of the inability to retain these functions [4].

European critical infrastructures are the critical infrastructures located in Member States whose disruption or destruction would have significant consequences for two or more Member States.

The Council of the European Union has adopted Directive 2008 / 114 / EC of 8 December 2008 [8] about the establishment and designation of European critical infrastructures, and assessing the need to improve their protection. This Directive mainly covers the energy and transportation sectors. The requirements of Directive 2008/114/EC have been incorporated into the national legislation of Bulgaria by Decree No.18 of the Council of Ministers of 01.02.2011 on the establishment and designation of European Critical Infrastructures in the Republic of Bulgaria, and the measures for their protection [9].

Critical infrastructures are taken into account when protecting the critical infrastructures resulting from human activity, technological threats and natural disasters, but priority is given to terrorist threats. Member States are ultimately responsible for the management of critical infrastructure protection mechanisms within their national borders.

There are a number of critical infrastructures in the Community whose disruption or destruction would have significant cross-border implications for more than one sector as a result of the interdependence of interconnected infrastructures. Such European critical infrastructures have been established and launched under a common procedure developed by the European Commission, with security requirements assessed according to a common minimum approach.

The critical infrastructure of Europe is divided into several sectors:

– Energy;
– Information and Telecommunication Systems;
– Water Resources;
– Food Industry;
– Healthcare;
– Financial Services;
– Law and Order;
– Public Services;
– Transportation Systems;
– Chemical and Nuclear Industries;
– Space Systems and Exploration.

– However, in Bulgaria, 19 sectors have been identified as critical, as follows [9]:

– Energy;
– Transportation;
– Telecommunications, including electronic communication networks, and information and communication infrastructure;
– Healthcare;
– Agriculture and Food;
– Environment;
– Finance and Banking;
– Defense;
– Justice, Public Order and Security;
– Economics;
– Education, Science and Technology;
– Natural Resources;
– Regional Development and Public Works;
– Tourism;
– Government and Social Governance;
– Disaster Protection;
– Cultural Heritage;
– Postal and Courier Services;
– Sports Facilities.

All of these sectors which have been identified as critical to the country are governed by the strategic documents on which the models for guaranteeing their security are based, and developed. The European Council meeting of June 2004 invited the Commission to prepare a common strategy for the protection of its critical infrastructure. On 20 October 2004, the Commission adopted the document "Protecting the Critical Infrastructure in the Fight against Terrorism" [8] with clear proposals for measures needed to improve the prevention, preparedness and response in Europe of terrorist attacks affecting the critical infrastructure. In its conclusions on the "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Program on the Effects of Terrorist Threats and Attacks", adopted in December 2004, the Council endorses the Commission's plan to propose a European Critical Infrastructure Protection Program (EPCIP) [9], and approved the creation of a Critical Infrastructure Warning Information Network (CIWIN) [10].

Taking these two measures defines the framework for the protection of EU infrastructure and accordingly defines the horizontal framework for the protection of EU critical infrastructure, explaining how EPCIP [9,10] (including CIWIN) can be put into effect.

The CIWIN initiative [9,10] is part of EPCIP, focusing in particular on the information sharing process between EU Member States, and addressing the IT system that supports this process.

Essentially, in the course of protecting the critical infrastructure, this means the identification of risk factors in the sector concerned. Critical infrastructure protection encompasses a set of activities designed to ensure the normal functioning, continuity and integrity of critical infrastructures to deter, reduce, mitigate or counteract threats, risks or vulnerabilities. The availability, integrity, and confidentiality model of security, integrity, and confidentiality is fully applicable to the security of critical information infrastructure.

In order to maximize the use of ICT infrastructures, and thus to make full use of the economic and social opportunities provided by the information society, all actors need to have high confidence in these infrastructures. This depends on various factors, the most important of which is to guarantee their high level of security and resilience. Diversity, openness, interoperability, usability, transparency, accountability, verifiability of different components and competition — these are key factors for improving security, and promoting the introduction of security products, processes and services.

The rapid pace of industrialization, as well as the use of artificial intelligence in the management and control of the production, transportation and storage of products and raw materials, necessitates an appropriate class of connectivity technologies.

These technologies have requirements for reliability, operation under extreme conditions, and protection that are many times higher than normal. This is due to the risks associated with the collapse of the systems that control critical infrastructures, such as nuclear power plants, gas transmission network, water supply and sewerage, and electricity transmission networks.

Typically, such networks have a mix of Scada [10] devices and Ethernet transmission. These two technologies must work seamlessly together, and must be well protected against cyber attacks aimed at disruption, theft, or manipulation of traffic.

The security of Scada systems is of particular importance in strategically important industrial and infrastructure sites — power plants, refineries, oil pipelines, treatment plants, manufacturing facilities, communication and transport infrastructures. With the advancement of technology, and the increasing number of Scada devices available online, the vulnerability of the sectors controlled by them has increased.

3. Industrial Control Systems. The industrial management system (ICS) is a generic term that covers several types of management systems, including Supervisory Management and Data Acquisition Systems (Scada) [11] (Figure 1), control systems (DCS), and other control systems such as PLCs, common in the industrial sectors and critical infrastructures. An ICS consists of combinations of components with specific controls (electrical, mechanical, hydraulic, pneumatic) that work together to achieve their purpose (e.g. production, material or energy transportation). The part of the system that mainly deals with the production of industrial products is called technological process. The part that controls the system includes a specification of the desired output or performance [12]. The control may be fully automated, or it may involve a person. Systems can be configured to work within an open cycle, closed cycle, and manual mode. For open-loop control systems, output is controlled by the settings set. In the closed loop control systems, output has such an effect on the input that it supports the desired purpose. In the manual mode, the system is entirely controlled by humans. The part of the system that is mainly concerned with maintaining the specification is called controller. A typical ICS system may contain multiple control cycles, human machine interfaces (HMI) [11], and remote diagnostics and support tools built using multiple network protocols. ICS industrial control processes are commonly used in sectors, such as electricity, dams, oil and natural gas, chemicals, transportation, pharmaceutical, pulp and paper, food and beverage industries (including automotive, aerospace, and durables). ICSs can largely be grouped by function into one or more of these three categories: overview, monitoring and management.

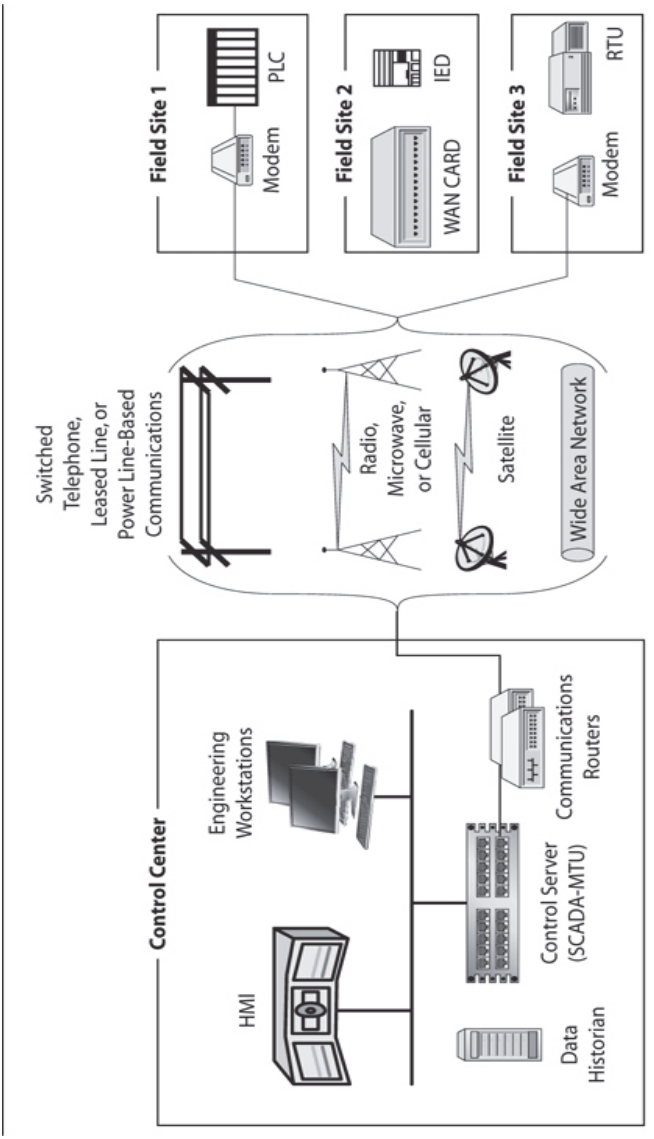

Fig. 1. General view of SCADA system

Труды СПИИРАН. 2019. Том 18 № 6. ISSN 2078-9181 (печ.)
ISSN 2078-9599 (онлайн) www.proceedings.spiiras.nw.ru

The Scada components [13] (Figure 2) system consist of sensors and actuators that are responsible for the collection of physical parametric data from field devices. These signals are typically stored in analogue format and converted through a remote terminal device, programmable logic controllers or an intelligent electronic device (IED). Once the data is converted, it is transmitted via a communication channel to the Scada control unit where the collected data is processed, and the operations are transmitted back to the field devices.

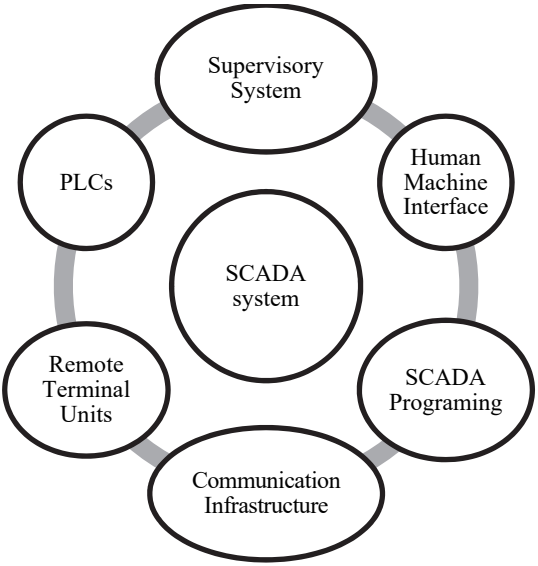

Fig. 2. Components of SCADA architecture

The Scada controller uses the HMI [14], which is responsible for submitting the collected data to operator in readable form. Further expansion of the architecture exists in situations where there is an operator outside the area of the industrial network, trying to control devices from remote locations. Communication between the field devices and the Scada host can be accomplished via dial-up, satellite, serial, radio, telephone, or WLAN. Also, specialized communication protocols such as DNP, DNP3, ICCP, Modbus and ProfiBus etc. have been integrated into the Scada network. As some of these protocols were in existence more than 20 years ago, when security was not a key factor in their construction, the main focus was on their effective operation, and not security.

With up to 4 layers (collection, conversion, communication and control) in the Scada system, it can be seen that each of the layers can be

used as an entry point to attack the system. A physical attack where the on-site devices are corrected by the attacker or the malicious person alters the data that is sent to the HMI. Some of the popular protocols that are still in use do not include authentication and encryption during their operation, and these shortcomings can be used to capture data that is transferred between devices. Insider exploitation errors or lack of proper access control can make HMI vulnerable, this can be used by a malicious attacker to interfere with industrial processes.

4. Security Issues within Scada Architecture.

4.1. HMI Vulnerability. An attacker can exploit the industrial Scada system by exploiting vulnerabilities that exist in the system's HMI [14, 15].

– Preset Name and Password — HMI component hacking can allow a remote attacker to control field devices. Exploitable vulnerabilities include embedded username and password in plain text in Java code used to design Web HMI;

– Validation of Field for Incorrect Input — also, incorrect encoding techniques can allow an attacker to execute requests through the Web HMI input field, leading to SQL injection attacks;

– Incorrect Authentication and Permission — bad authentication techniques are a door in the system. For example, the lack of a two-factor system for certification in critical infrastructure leaves an attacker unable to gain access to the system without much effort.

4.2. Zero Day Exploits. Unidentified vulnerabilities by system software vendors are one of the most common threats exploited by Scada network attackers. Due to the nature of the vulnerability, an attacker can infiltrate the system by performing intelligence, scanning and logging without being detected.

4.3. PLC Vulnerabilities. PLCs, sensors, and actuators serve as aggregators of data in the industrial field. It is possible for the attacker to take control of the PLC by exploiting vulnerabilities, and then directly or indirectly intervening in industrial processes. Attacking PLC firmware vulnerabilities by an attacker can provide direct access to the sensors and actuators of the field.

4.4. Social Engineering. Cyber-attackers can use social engineering methods to break into the web. Checking IoT databases such as shodan.io for device username and passwords is one way to learn the web. Email spear phishing methods can also be considered an entry point into the corporate network if the attacker's intention is to bring malware into the network. Hijacking an insider to physically connect a device (such as USB, disk drive) to distribute malware is also possible.

4.5. Inadequate Physical Security. The field devices themselves are responsible for the industrial process, and inappropriate physical security procedures can allow an unauthorized attacker to gain physical access to the devices. As a result — although Scada monitoring includes an alarm due to the infectious data it has received — it will be quite difficult for the situation to be remedied except by physical means.

4.6. Vulnerabilities of the Scada Protocol. Most of the common protocols used on Scada networks are for operational efficiency, not security. They do not include authentication mechanisms used in traditional IT systems that are used to authenticate the sender or recipient of the data, thereby allowing attackers to compromise the integrity and confidentiality of sensor values.

4.7. Corporate Network Connection. Earlier Scada systems relied on point-to-point networks. To scale the Scada networks to fit current organizational needs, Scada systems have been connected to the corporate network through a secure gateway. Corporate networks operate as computer networks; they are susceptible to attacks such as SQL injection, phishing, spear phishing, and other vulnerability exploits.

5. Tree-based Security Breach Risk Analysis. Attack trees were introduced by Schneier [29] as a way of officially analyzing the security of systems and subsystems based on various attacks. Schneier's work is remarkable, as it is the first time that this information security approach has been implemented. The purpose of the attack is the root of the tree, and the various ways of carrying out the attack are the leaves, with connections through nodes AND and OR.

Figure 3 shows an image of a target tree. The attack tree consists of OR nodes, AND nodes, and Leaf nodes. The topmost node is the root node, which shows the overall purpose of the hacker. The top node is decomposed into several sub-goals that consist of other nodes and leafs. The OR node indicates that the attack can be performed by completing 1 or more sub-targets. For example, the OR target #1 can be achieved either through subgroup #1a, or subgroup #1b. The AND node indicates that the attack can be carried out by completing all the sub-goals. For example, goal AND #2 can be achieved by performing subgroup #2a and subgroup #2b.

Moore et al. [19] describe and illustrate an approach for documenting attacks against software systems that use structured and reusable attack tree information. Analysts can then use the approach to document and identify common attack patterns, and then modify attack trees to improve security development.

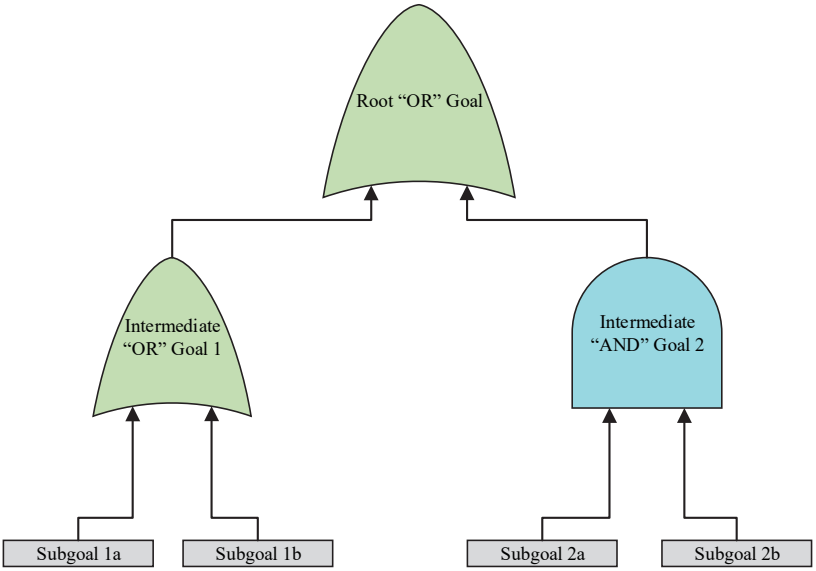

Fig. 3. Example Tree

Recently, attack trees have been applied to the Scada communication system[29]. The authors have identified eleven targets of attackers and related security vulnerabilities in the specification and development of a typical Scada system:

1. Easing the access to the Scada system;
2. Identifying the Modbus device;
3. Disconnecting the master and slave modules, or breaking the Master-Slave rule;
4. Disabling subordinates;
5. Reading data from subordinates;
6. Recording data in subordinates;
7. Programming of subordinates;
8. Compensation of subordinates;
9. Disabling the Main Module;
10. Main Module Data Recording;
11. Modifying the Master Module.

6. Methodology of the Analysis. Figure 4 shows a schematic overview of the methodology for generating attacking trees, and a description of the workflow from the adoption of a system model to the categorization of opportunities for threat level. Secure-Tree Modeling Tool [2] by Amenaza Technologies Ltd. used in developing the attack tree.

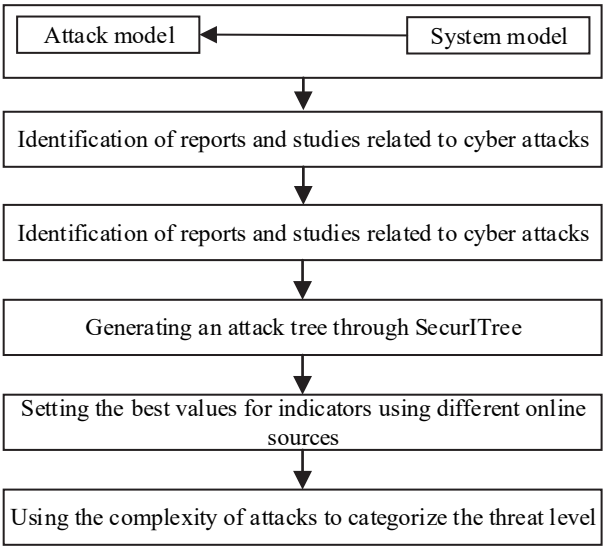

Fig. 4. Methodology of the Analysis

7. Scada System Attack. The purpose of the attack is to terminate fuel operations [20]. Upon successful attack, the attacker can change the Fuel Manager Database (FMD) protection data, change the real-time HMI data, crash the FMD hard drive, submit a fake fuel company report, and violate the FMD communication.

7.1. Indicators. An attacker needs a variety of resources to attack. Four different indicators are considered below:

– accessibility — accessibility is measured by how easily an attacker can access a restricted system;

– sight — sight is the measure of how secretly an attacker can perform an attack without being noticed. Visibility measurement comes from the mystery of the attack from the planning stage to intelligence, until the attack is successfully completed;

– technical ability — technical ability is the measure of how easily an attack can be done. This is related to the level of the attacker, the level of expertise and specialization that are taken into account in determining the technical capabilities of the attacker;

– breakthrough time — breakthrough time is a measure of how long it will take from planning to the final execution of an attack.

The attack tree is built from the end leaves to the nodes until the attacker reaches his target, which is the root node. Table 1 shows how to

select Leaf attack tree nodes and how OR and AND nodes are calculated. For OR nodes, all Leaf nodes are considered in the attack. This means that the number of Leaf nodes added to the OR nodes affects the number of attack scenarios generated.

Table 1. Node range

Indicator name	LOGICAL OR	LOGICAL AND	Range
Accessibility	Minimum Peaks: The tree selects and examines each of the nodes for each attack.	Minimum Peak Value: The value of Leaf nodes with the highest system access restriction is selected to move to the root node. For example, in an attack consisting of a high-access (unrestricted) node and a medium-access (moderate-access) node, the value of a moderate node rises on the tree, being a more complex node.	1-3
Landmark	Minimum Peaks: The tree selects and examines each of the nodes for each attack.	Minimum Peak Value: The value of the leaf node with the most inconspicuous attack is selected to move to the root node. This is because the lower the value of the leaf node, the less noticeable the attack.	1-5
Technical ability	Minimum Peaks: The tree selects and examines each of the nodes for each attack.	Maximum Peak Value: The value of Leaf nodes with the highest technical ability is selected to move to the primary node. This is because the higher the score, the higher the technical ability required to perform the attack. If one of the leaf attack nodes is a combination of very difficult attacks, then the attack must also have high technical ability.	1-5
Breakthrough time	Minimum Peaks: The tree selects and examines each of the nodes for each attack.	Maximum Peak Value: The value of the Leaf node with the most time to perform the attack is selected to move to the root node.	1-5

7.2. Scada System Attack Scenario. Many attack nodes describe elements of an advanced persistent threat (APT). The anatomy of APT attacks describes social engineering, spear phishing, malware, mapping, escalation of privileges, and networking. APTs are designed to be difficult to see in network traffic as they move from one host to another. For example, Trojan, Rootkits, and Backdoors are designed in such a way that they can maintain a low profile in the system. Figure 5 gives an overview to all nodes of the attack.

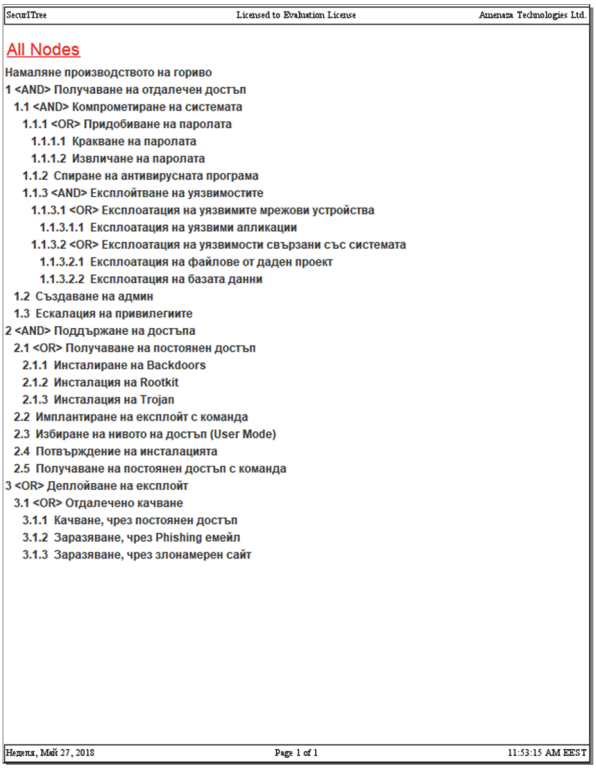

Fig. 5. All nodes of the attack in full view

7.3. Scada System Attack Scenario — analysis using complexity index SecurITree software provides a tool that allows you to identify threat profiles. Attack scenarios that fall into threat level 1 have the highest level of attack complexity (Table 2). The level of complexity of attacks decreases from threat level 1 to threat level 5. While attacks under threat level 1 are the most complex, threat level 5 can lead to an attack against healthcare infrastructure with less complexity and better results. In the Scada attack scenario, it can be seen that only attackers under threat 1 and 3 can carry out the attack.

Table 2. Assigning weight to each of the nodes

№	Attack nodes	Technical ability	Accessibility	Landmark	Attack time
1	Create admin	4	3	4	1
2	Escalation of privileges	4	3	2	1
3	Password cracking	3	3	3	2
4	Password retrieval	4	3	4	4
5	Stopping the antivirus program	4	2	4	2
6	Operation of vulnerable applications	4	3	3	2
7	Operation of files from a project	4	2	3	2
8	Operation of the database	5	2	4	3
9	Installing Backdoors	3	2	2	2
10	Rootkit installation	3	2	2	2
11	Trojan installation	3	2	2	3
12	Implanting an exploit with a command	2	3	3	1
13	Selecting the Access Level (User Mode)	3	3	3	2
14	Selecting the Access Level (User Mode)	2	2	3	1
15	Get permanent access with a command	3	3	4	2
16	Upload, with permanent access	2	3	4	3
17	Contamination by Phishing Email	4	1	2	2
18	Infection through a malicious site	4	1	2	2

An attack causing reduced WPAFB combustion processing utilizes all the characteristics of a sophisticated attack. There are elements of social engineering, APT, insubordination, remote administration, and exploitation of Zero-Day vulnerabilities in the attack being analyzed. This gives the total SI score for this attack to be 5. Which is the highest SI score obtained. An additional illustration is shown in Table 3.

Table 3. Determination of SI coefficient for SCADA system

Types of features	Attack nodes	SI
Social Engineering	Infection by Phishing email	1
Remote Administration	Backdoors installation, Rootkit installation, command implant implantation, installation confirmation	1
Landmark	Antivirus suspension, escalation of privileges, exploitation of vulnerable applications, installation of Rootkit	1
Zero-Day Vulnerabilities	Database vulnerability	1
APT	Backdoors installation, Rootkit installation, admin creation	1
		All = 5

8. Results of the Attack on Scada. The minimum level of threat required to attack an industrial Scada infrastructure is threat level 3. Due to the AND function of the root node, all attacks must be made to achieve an attack from any of the threat levels. Threat Level 3 has 36 scenarios that are the same as the total number of scenarios generated by the attack tree. This means that an attacker with high technical skills, limited access to the system, an increased level of insubordination, and ready to devote months to years to planning and executing the attack, can make a successful attack. The maximum level of threat required to attack an industrial Scada system for generating a physical result is threat level 1. An attacker with a level 1 threat

will also be able to execute all 36 attacks on a Scada system attack, and he does so with unlimited access to the system.

Although a third-level attacker can execute an attack, the result of the analysis indicates that an attacker with a threat level 2 cannot execute the attack. This is because the attacker with threat level 2 has only an average technical level of cyber knowledge, although the indicators of incompleteness and access are high. For this reason, it can be concluded that the attacker's technical ability is one of the most important indicators when analyzing an attacker's capabilities.

There are two types of errors for evaluating IDS, for each possible test value: false positive (FP) and false negative (FN). FP occurs when an event is intended to be intrusive, but is actually normal, whereas FN occurs when a truly intrusive event occurs without being recognized as one. On the other hand, the true positive (TP) measures the proportion of true positives that are correctly identified as such, while the true negative (TN) measures the proportion of negatives that are correctly identified as such.

The performance of each classifier can be quantified using measures of measurement of detection rate (DR) and overall accuracy (OA). DR shows the percentage of true breaks that were successfully detected:

$$DR = \frac{TP}{TP + FN} \times 100\%.$$

OA is calculated as the total number of correctly classified infiltrations divided by the total number of observations:

$$OA = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%.$$

Effective IDS requires a high degree of DR and OA while maintaining low levels of false alarms. Accuracy is critical to developing an effective IDS, since high FP speeds or low DRs will render it practically useless.

The Table 4 below lists data from a standard IDS system that is used to protect the Scada information infrastructure under study.

Table 4. Simulation results for DDoS attack detection

Attack (% from affected endpoints)	FP %	FN %	OA
1	1.2	1.1	60.1
5	1.3	1.2	60.05
10	1.5	1.6	60.13

Table 4 (continued)

15	1.7	1.8	60.7
20	1.9	2	62.03
25	2.1	2.3	61.83
30	2.4	2.5	62.38
35	2.6	2.7	62.58
40	3.1	3	62.68
45	3.2	3.4	62.7
50	3.3	3.7	63.65
55	3.5	3.8	65.08
60	3.7	3.9	66.05

From the graph above (Figure 6), it is visible that the system becomes more accurate with the increase of the relevant percentage. More affected endpoints lead to more accurate results. If the attack is smaller and targeted at a specific endpoint, it will be very difficult to detect it. In the course of this experiment, the gateway capability of the Scada system in/out point of the network was also recorded (Figure 7).

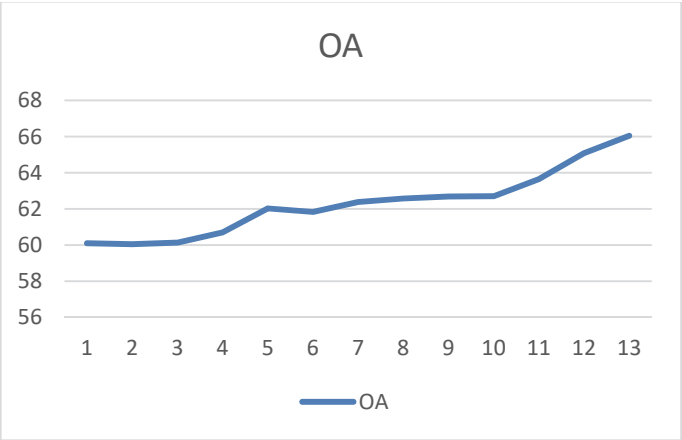

Fig. 6. Overall accuracy

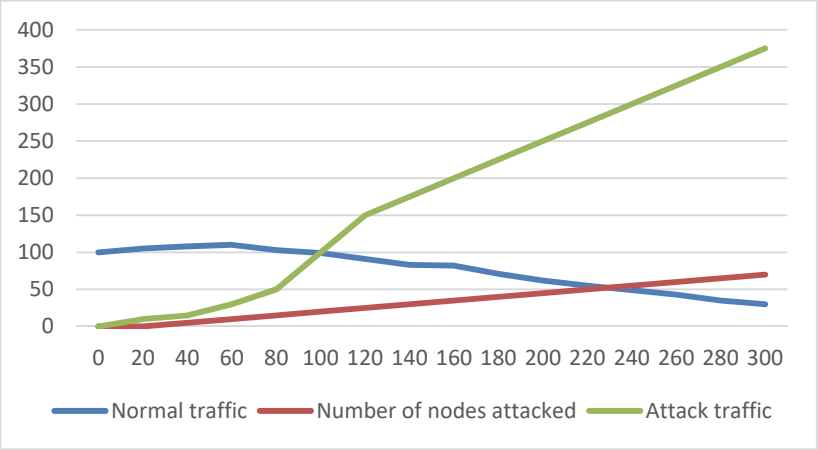

Fig. 7. Network traffic

9. Conclusion. Strategic planning for critical infrastructure protection requires the coordination and coordination of actions taken across time and space. Critical infrastructure protection planning needs to be based on a specific platform. It is created with the help of relevant information, mainly of a regulatory nature — laws, decrees, directives, regulations, instructions and other documents.

The real-time cybersecurity of continuous systems requires an overall view and comprehensive understanding of network security, control theory, and the physical system. Ultimately, all viable technical solutions and research guidelines for the provision of Scada systems must be related to computer security, communications network and control engineering. The idea itself of looking into the problem within the context of performance control has its foundations. There are two types of errors for evaluating by the Intruder Detection System, for each possible test value: false positive and false negative. Effective Intruder Detection System requires a high degree of detection rate and overall accuracy, while maintaining low levels of false alarms. Accuracy is critical to developing an effective Intruder Detection System, since high false positive speeds or low detection rates will render it practically useless. The experiments show that with increasing attack traffic at multiple entry points the inrtuder detection system becomes more accurate. More affected endpoints lead to more accurate results. If the attack is smaller and targeted at a specific endpoint, it is very difficult to detect it. The damage increases when adequate attention to the various devices involved in the detection process is not provided. Each of these devices has a specific structure (software and hardware) and thus requires individual and specific protection.

The attacker's technical ability is one of the most important indicators when analyzing attacker's capabilities. This means that an attacker with high technical skills, even with limited access to the system, but ready to devote months to years in planning and executing the attack, can make a successful attack.

The future work of the team will include a more in-depth study of the cyber-physical connections of the individual elements and the various participants in a critical information infrastructure, as well as the application of active polling in order to reduce the rate of cyber attacks.

References

1. Almalawi A. et al. An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. Computers & Security. 2014. vol. 46. pp. 94–110.
2. Amenaza Technologies Limited. Available at: https://www.amenaza.com/faq.php (accessed: 25.08.2019).
3. Byres E.J, Franz M., Miller D. The Use of Attack Trees in Assessing Vulnerabilities in SCADA System. Proceedings of the International Infrastructure Survivability Workshop (IISW'04). 2004. pp. 3–10.
4. Dochev D., Pavlov R., Paneva-Marinova D., Pavlova L. Towards Modeling of Digital Ecosystems for Cultural Heritage. *Digital Presentation and Preservation of Cultural and Scientific Heritage*. 2019. vol. 9. pp. 77–88.
5. IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control. Institute of Electrical and Electronics Engineers. 1987.
6. IoT And SCADA: Is One Going To Replace The Other? Available at: https://www.iotnxt.com/2018/07/18/iot-or-scada/ (accessed: 25.08.2019).
7. Oficialen sajt Microsoft Story Lab [Official web site of Microsoft Story Lab]. Available at: https://news.microsoft.com/stories/cloud-security (accessed: 25.08.2019). (In Bulg.).
8. EU Directive 2008/114/EC of 8 December 2008. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG (accessed: 25.08.2019).
9. Naredba za reda za ustanovyavaneto i oznachavaneto na evropejski kritichni infrastrukturi v republika B"lgariya i merkite za tyahnata zashchita [Ordinance on the procedure for the establishment and designation of European Critical Infrastructures in the Republic of Bulgaria and the measures for their protection]. Available at: https://www.lex.bg/laws/ldoc/2135839567 (accessed: 25.08.2019). (In Bulg).
10. Communication from the Commission on a European Programme for Critical Infrastructure Protection. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786 (accessed: 25.08.2019).
11. Industrialen Ethernet i SCADA [Industrial and SCADA]. Available at: https://radesol.com/bg/industrialen-ethernet-scada/ (accessed: 25.08.2019).
12. Xing L., Demertzis K., Yang J. Identifying data streams anomalies by evolving spiking restricted Boltzmann machines. *Neural Computing and Applications*. 2019. pp. 1–15.
13. Lecture notes. Available at: https://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/lectures.html (accessed: 25.08.2019).
14. Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, NIST 2018. Available at: https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final (accessed: 25.08.2019).
15. Lee M.R., Assante M.J., Conway T. ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Cyber Attack. SANS ICS. 2014. 15 p. Available at: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf (accessed: 25.08.2019).
16. Malaviya S. SCADA Cybersecurity Framework. *ISACA Journal.* 2014. vol. 1. 5 p.

17. Eriksson M., Johansson T.T. An Example of a Man-in-the-Middle Attack Against Server Authenticated SSL-Sessions. International conference on applied cryptography and network security. 2003.
18. Moore A.P., Ellison R.J., Linger R.C. Attack Modeling for Information Security and Survivability. Carnegie-Mellon University. 2001. 32 p.
19. Iliev O. Radar Charts: A Novel Means to Explore the Relationship Between QoS and QoE.
20. Paneva-Marinova D., Stoikov J.S., Pavlova L.R., Luchev D.M. [System Architecture and Intelligent Data Curation of Virtual Museum for Ancient History]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2019. vol. 18(2). pp. 444–470.
21. Radvanovsky R., Brodsky J. Handbook of SCADA/Control Systems Security. CRC Press. 2013.
22. Trifonov R. et al. Increasing the level of network and information security using artificial intelligence. Fifth International Conference on Advances in Computing, Communication and Information Technology. 2017. pp. 83–88.
23. Trifonov R., Yoshinov R., Jekov B., Pavlova G. Methodology for Assessment of Open Data. *International Journal of Computers*. 2017. Issue 2. pp. 28–37.
24. Trifonov R., Yoshinov R., Jekov B., Pavlova G. E-government assessment. *International Journal of Development Research*. 2017. vol. 07. pp. 14874–14881.
25. Trifonov R., Yoshinov R., Pavlova G., Tsochev G. Artificial neural network intelligent method for prediction. AIP Conference Proceedings. vol. 1872. no. 1. pp. 020021.
26. Trifonov R. et al. A Survey of Artificial Intelligence for Enhancing the Information Security. International Journal of Development Research. 2017. vol. 7. no. 11. pp. 16866–16872.
27. Trifonov R. et al. Conceptual model for cyber intelligence network security system. *International Journal of Computers*. 2017. vol. 11. pp. 85–92.
28. Krutz R.L. Securing SCADA systems. Wiley Publishing, Inc. 2006. 240 p.
29. Schneider Electric. Available at: https://www.se.com/ww/en/product-category/6000-telemetry-and-remote-scada-systems/ (accessed: 25.08.2019).
30. Morris T., Gao W. Industrial control system traffic data sets for intrusion detection research. International Conference on Critical Infrastructure Protection. 2014. pp. 65–78.
31. Fillatre L., Nikiforov I. A statistical method for detecting cyber/physical attacks on SCADA systems. 2014 IEEE Conference on Control Applications (CCA). 2014. pp. 364–369.

Tsochev Georgi Rumenov — Ph.D., Chief Assistant Professor, Laboratory of Telematics, Bulgarian Academy of Sciences (BAS). Research interests: computer science, computer networks and communication, neural networks, deep learning, application of mathematics and informatics in cybersecurity. The number of publications — 25. gtsochev@gmail.com; 8 bl., Acad. Georgi Bonchev Str., 1113, Sofia, Bulgaria; office phone: +359895589861.

Yoshinov Radoslav Dakov — Ph.D., Professor, Head of Laboratory, Laboratory of Telematics, Bulgarian Academy of Sciences (BAS). Research interests: computer science, medical systems, computer networks and communication, deep learning, cybersecurity, E-Government cybersecurity of computer networks. The number of publications — 191. yoshinov@cc.bas.bg; 8 bl., Akad. G. Bonchev Str., 1113, Sofia, Bulgaria; office phone: +359888627190.

Iliev Oleg Petrov — Junior Researcher, Laboratory of Telematics, Bulgarian Academy of Sciences (BAS). Research interests: information technologies, computer science, IT components to support education process. The number of publications — 6. iliev.oleg@gmail.com; 8 bl., Akad. G. Bonchev Str., 1113, Sofia, Bulgaria; office phone: +359884381052.

Acknowledgements. This research is supported through IKT in NOS program of MES.

УДК 006.72 **DOI** 10.15622/sp.2019.18.6.1333-1356

Г.Р. Цочев, Р.Д. Йошинов, О.П. Илиев

ОСНОВНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ СЕТЕЙ НА ОСНОВЕ СИСТЕМ SCADA

Цочев Г.Р., Йошинов Р.Д., Илиев О.П. **Основные проблемы защиты критической инфраструктуры сетей на основе систем SCADA.**

Аннотация. Критические инфраструктуры и оперативная совместимость составляющих ее информационно-ресурсных компонентов — главная составляющая жизненного цикла инфраструктуры. Поскольку системы диспетчерского контроля и сбора данных ((анг. Supervisory Control and Data Acquisition — SCADA) являются частью критической инфраструктуры, их киберзащита особенно важна на стратегических объектах, таких как электростанции, нефтеперерабатывающие заводы, нефтепроводы, очистные сооружения, производственные объекты, транспорт и так далее. Наряду с развитием технологий и онлайн доступности устройств систем SCADA, также увеличилась уязвимость подконтрольных им секторов. В мире Интернета вещей конечные устройства вызывают новую волну возможных уязвимостей в SCADA, так как они подвержены атакам и взломам и через них можно получить доступ к системе. В Европейском сообществе существует ряд критически важных инфраструктур, нарушение или разрушение которых может иметь значительные по масштабу трансграничные последствия для более чем одного сектора как результатвзаимозависимости взаимосвязанных инфраструктур. Такие европейские критические инфраструктуры были созданы и запущены в соответствии с разработанной Европейской комиссией общей процедурой, включающей в себя оценку требований безопасности, с учетом общего минимального подхода.

Рассматриваются критические инфраструктуры Европейского Союза и Болгарии. Посредством структуры системы SCADA были проанализированы уязвимости и различные возможности для ее атаки. В качестве примера рассмотрен конкретный случай, на премере деревьев атак, и полученные результаты были обобщены и визуализированы. Проанализированы последствия и сделаны соотвествующие выводы.

Ключевые слова: критическая инфраструктура, SCADA, дерево атаки, киберзащита, сетевая информационная защита.

Цочев Георги Руменов — Ph.D., главный ассистент, лаборатория телематики, Болгарская академия наук (БАН). Область научных интересов: информатика, компьютерные сети и связь, нейронные сети, глубинное обучение, применение математики и информатики в кибербезопасности. Число научных публикаций — 25. gtsochev@gmail.com; ул. Академика Георги Бончев, 8 bl., 1113, София, Болгария; р.т.: +359895589861.

Йошинов Радослав Даков — Ph.D., профессор, заведующий лабораторией, лаборатория телематики, Болгарская академия наук (БАН). Область научных интересов: информатика, медицинские системы, компьютерные сети и связь, глубинное обучение, кибербезопасность, кибербезопасность компьютерных сетей электронного правительства. Число научных публикаций — 191. yoshinov@cc.bas.bg; ул. Академика Георги Бончев, 8 bl., 1113, София, Болгария; р.т.: +359888627190.

Илиев Олег Петров — младший научный сотрудник, лаборатория телематики, Болгарская академия наук (БАН). Область научных интересов: информационные технологии, информатика, ИТ-компоненты для поддержки учебного процесса. Число научных публикаций — 6. iliev.oleg@gmail.com; ул. Академика Георги Бончев, 8 bl., 1113, София, Болгария; р.т.: +359884381052.

Поддержка исследований. Работа выполнена при финансовой поддержке программы ИКТ в НОС, МОН.

Литература

1. *Almalawi A. et al.* An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems // Computers & Security. 2014. vol. 46. pp. 94–110.
2. Amenaza Technologies Limited. URL: https://www.amenaza.com/faq.php (дата обращения: 25.08.2019).
3. *Byres E.J, Franz M., Miller D.* The Use of Attack Trees in Assessing Vulnerabilities in SCADA System // Proceedings of the International Infrastructure Survivability Workshop (IISW'04). 2004. pp. 3–10.
4. *Dochev D., Pavlov R., Paneva-Marinova D., Pavlova L.* Towards Modeling of Digital Ecosystems for Cultural Heritage // Digital Presentation and Preservation of Cultural and Scientific Heritage. 2019. vol. 9. pp. 77–88.
5. IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control // Institute of Electrical and Electronics Engineers. 1987.
6. IoT And SCADA: Is One Going To Replace The Other? URL: https://www.iotnxt.com/2018/07/18/iot-or-scada/ (дата обращения: 25.08.2019).
7. Официален сайт Microsoft Story Lab. URL: https://news.microsoft.com/stories/cloud-security (дата обращения: 25.08.2019).
8. EU Directive 2008/114/EC of 8 December 2008. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG (дата обращения: 25.08.2019).
9. Наредба за реда за установяването и означаването на европейски критични инфраструктури в република България и мерките за тяхната защита. URL: https://www.lex.bg/laws/ldoc/2135839567 (дата обращения: 25.08.2019).
10. Communication from the Commission on a European Programme for Critical Infrastructure Protection. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786 (дата обращения: 25.08.2019).
11. Индустриален Ethernet и SCADA. URL: https://radesol.com/bg/industrialen-ethernet-scada/ (дата обращения: 25.08.2019).
12. *Xing L., Demertzis K., Yang J.* Identifying data streams anomalies by evolving spiking restricted Boltzmann machines // Neural Computing and Applications. 2019. pp. 1–15.
13. Lecture notes. URL: https://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/lectures.html (дата обращения: 25.08.2019).
14. Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, NIST 2018. URL: https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final (дата обращения: 25.08.2019).
15. *Lee M.R., Assante M.J., Conway T.* ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Cyber Attack // SANS ICS. 2014. 15 p. URL: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf (дата обращения: 25.08.2019).
16. *Malaviya S.* SCADA Cybersecurity Framework // ISACA Journal. 2014. vol. 1. 5 p.
17. *Eriksson M., Johansson T.T.* An Example of a Man-in-the-Middle Attack Against Server Authenticated SSL-Sessions // International conference on applied cryptography and network security. 2003.
18. *Moore A.P., Ellison R.J., Linger R.C.* Attack Modeling for Information Security and Survivability // Carnegie-Mellon University. 2001. 32 p.
19. *Iliev O.* Radar Charts: A Novel Means to Explore the Relationship Between QoS and QoE.
20. *Paneva-Marinova D., Stoikov J.S., Pavlova L.R., Luchev D.M.* System Architecture and Intelligent Data Curation of Virtual Museum for Ancient History // Труды СПИИРАН. 2019. vol. 18(2). pp. 444–470

21. *Radvanovsky R., Brodsky J.* Handbook of SCADA/Control Systems Security // CRC Press. 2013
22. *Trifonov R. et al.* Increasing the level of network and information security using artificial intelligence // Fifth International Conference on Advances in Computing, Communication and Information Technology. 2017. pp. 83–88.
23. *Trifonov R., Yoshinov R., Jekov B., Pavlova G.* Methodology for Assessment of Open Data // International Journal of Computers. 2017. Issue 2. pp. 28–37.
24. *Trifonov R., Yoshinov R., Jekov B., Pavlova G.* E-government assessment // International Journal of Development Research. 2017. vol. 07. pp. 14874–14881.
25. *Trifonov R., Yoshinov R., Pavlova G., Tsochev G.* Artificial neural network intelligent method for prediction // AIP Conference Proceedings. vol. 1872. no. 1. pp. 020021.
26. *Trifonov R. et al.* A Survey of Artificial Intelligence for Enhancing the Information Security // International Journal of Development Research. 2017. vol. 7. no. 11. pp. 16866–16872.
27. *Trifonov R. et al.* Conceptual model for cyber intelligence network security system // International Journal of Computers. 2017. vol. 11. pp. 85–92.
28. *Krutz R.L.* Securing SCADA systems // Wiley Publishing, Inc. 2006. 240 p.
29. Schneider Electric. URL: https://www.se.com/ww/en/product-category/6000-telemetry-and-remote-scada-systems/ (дата обращения: 25.08.2019).
30. *Morris T., Gao W.* Industrial control system traffic data sets for intrusion detection research // International Conference on Critical Infrastructure Protection. 2014. pp. 65–78.
31. *Fillatre L., Nikiforov I.* A statistical method for detecting cyber/physical attacks on SCADA systems // 2014 IEEE Conference on Control Applications (CCA). 2014. pp. 364–369.