INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2023, VOL. 69, NO. 3, PP. 475-483
Manuscript received January 10, 2023; revised July, 2023. DOI: 10.24425/ijet.2023.146495

Development of an Information Security System Based on Modeling Distributed Computer Network Vulnerability Indicators of an Informatization Object

Valerii Lakhno, Zhuldyz Alimseitova, Yerbolat Kalaman, Olena Kryvoruchko, Alona Desiatko, and Serhii Kaminskyi

***Abstract*—A methodology for development for distributed computer network (DCN) information security system (IS) for an informatization object (OBI) was proposed. It was proposed to use mathematical modeling at the first stage of the methodology. In particular, a mathematical model was presented based on the use of the apparatus of probability theory to calculate the vulnerability coefficient. This coefficient allows one to assess the level of information security of the OBI network. Criteria for assessing the acceptable and critical level of risks for information security were proposed as well. At the second stage of the methodology development of the IS DCN system, methods of simulation and virtualization of the components of the IS DCN were used. In the course of experimental studies, a model of a protected DCN has been built. In the experimental model, network devices and DCN IS components were emulated on virtual machines (VMs). The DCN resources were reproduced using the Proxmox VE virtualization system. IPS Suricata was deployed on RCS hosts running PVE. Splunk was used as SIEM. It has been shown that the proposed methodology for the formation of the IS system for DCN and the model of the vulnerability coefficient makes it possible to obtain a quantitative assessment of the levels of vulnerability of DCN OBI.**

***Keywords*—information security; informatization object; distributed computing network; mathematical model; vulnerability coefficient; virtualization; IDS; SIEM**

I. Introduction

In the context of a constantly changing landscape of information security (hereinafter referred to as IS) threats of companies (hereinafter referred to as informatization objects or OBI), as well as as the tactics and strategies of computer intruders improve, information security specialists rely heavily on the efficiency and reliability of information security systems (hereinafter referred to as ISS). The main task of such information security facilities is to prevent the leakage of information (often confidential) outside information systems. As shown in a number of studies [1], [2], [3], most information security incidents are associated with information leaks that occur as a result of human errors. And only about 25% of leaks are caused by the actions of hackers, insiders or malicious intent of information systems users.

It is clear that both insiders and external violators will try to overcome the means of information security (or information security system - ISS). It is especially relevant during targeted attacks. The outcome of such a confrontation between the attacking side and the defending side depends on many factors. As a result, it is impossible to guarantee the success of protection in advance, no matter how perfect the information security system of the informatization object (hereinafter referred to as OBI) is.

Note that as both the number [4], [5] and the complexity of carrying out attacks [6], [7] become more complex, modern multiloop IPSs are designed to solve additional problems. Such auxiliary tasks may include:

1) prevention of cases of transmission of unwanted information both inside and outside the information system;
2) prevention of situations when personnel use information system resources for their own personal purposes;
3) traffic monitoring and optimization of a data transmission channels load within a distributed computer network (hereinafter referred to as DCN) of the OBI and/or its information system;
4) avoidance of the situations when staff or third parties try to transmit unsolicited information (for example, spam or excessive amounts of information);
5) archivation of forwarded messages, which is necessary, for example, in a situation when a deeper analysis of an information security incident is required;
6) monitoring the presence of personnel in the workplace.

In some cases, auxiliary tasks solved by the information security system can be extremely important for preventing information leakage. For example, when it comes to identifying an insider in a company.

Nowadays, whenever one talks about protection against external IS violators, intrusion detection systems have become

Valerii Lakhno is with National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine (e-mail: lva964@nubip.edu.ua).

Zhuldyz Alimseitova and Yerbolat Kalaman is with Satbayev University, Almaty, Kazakhtan (e-mail: zhuldyz_al@mail.ru, kalaman.erbolat@gmail.com).

Olena Kryvoruchko, Alona Desiatko and Serhii Kaminskyi are with Kyiv National University of Trade and Economics, Kyiv, Ukraine (e-mail: ev_kryvoruchko@ukr.net, desyatko@gmail.com, s.kaminskyj@knute.edu.ua).

an integral part of the IS DCN contours of many companies and organizations. Moreover, both intrusion detection systems (IDS) and intrusion prevention systems (IPS) or combined IDS / IPS solutions are used in the previously mentioned case. In the latter case, IDS / IPS systems, which are software and hardware, serve to protect the network from unauthorized access.

In order to implement a systematic approach to ensuring the information security of the OBI network, it is not enough for the protection side to use only an arsenal of technical information protection means. It is necessary to use scientific methods at the design stage of such an information security system. Such scientific methods include, for example, mathematical or simulation modeling of information security systems and processes for a particular OBI. The priority goal of such modeling is to search for the optimal solutions related to the management of the OBI information security system. And besides, as a rule, additional tasks arise, for example, related to evaluating the effectiveness of the certain information security mechanisms usage, for example, the IDS / IPS already mentioned above. The entire process of modeling the ISS for a specific OBI can be conditionally divided into two components:

1) development of the models, for example, mathematical, physical or simulation;
2) implementation of models in order to obtain the necessary characteristics of the information security system.

All of the above mentioned determines the relevance of the research topic. Namely, the development of a methodology for the development of the DCN IS system based on mathematical and simulation modeling of the OBI vulnerability indicators.

II. Literature review

When it comes to an information security system for a particular OBI creation, the defense side usually faces one of two possible situations.

In the first case, it is necessary to create an information security system for OBI from scratch. In fact, the IS system is being developed without relying on existing solutions at the protected object, but with realization of the importance of an integrated approach for IS of the OBI. In the second case, OBI already has some means of information security. And the defense side is tasked to increase its effectiveness. For example, it can be achieved by the optimization of the ISS composition. As well as redistribution of the available funds in such a way as to protect the most valuable information OBI assets. Note that the second variant is much more common [8], [9], [10], [11]. Despite the disappointing statistics on cyber-attacks [12], [13], OBI management often does not pay due attention to information security issues until it encounters problems caused by either weak protection of its information assets or the actual absence of it. However, if the OBI owners face real problems caused by the improper state of information security, they are ready for large financial investments in information security. And the priority is to prevent the recurrence of such situations.

As shown in [14], the achievement of a given level of OBI IS depends on the successful solution of a set of interrelated tasks. Such tasks may include, for example, technical and technological, financial, organizational and other tasks that are solved during the development and implementation of the information security system.

The models proposed in [15], [16] have become classical in solving the problem of assessing the feasibility of financial investments (investments) in information security. However, it should be noted that both the basic model presented in these works and its supplemented modifications, for example, [17], have certain drawbacks. In particular, it was shown in [18] that the models [15], [16], [17] are predominantly based on restrictive assumptions. Such models do not make it possible to evaluate the dynamic aspects of investment in OBI information security. Namely, the dynamically changing landscape of cybernetic threats is the key moment in the formation of the DCN information security system for the OBI. And besides, dynamically changing threats also affect the vulnerability indicators of the DCN.

Risks and vulnerability assessment in the IS loops of the OBI is one of the key topics in the works of many researchers [18], [19], [20], [21], [22], [23], dealing with the IS vulnerabilities and threats assessment.

As shown in [19], [20], [21], in order to determine the OBI IS indicators, it is sufficient to know the probabilistic characteristics of threats and the possible ISS mechanisms effectiveness. The considered above works [7], [10], [16], [21], [22], [23] indicate that a purposeful organization requires to counter both existing and potentially new threats in the field of information security threat counter processes. Moreover, the implementation of these processes should include the usage of all available information security tools.

Thus, based on the foregoing, it can be stated that the task of methodology development for the formation of an IS system based on modeling the vulnerability indicators of DCN as an integral part of most modern OBI remains relevant.

III. The purpose and objectives of the study.

Development of a methodology for the formation of an information security system based on modeling the vulnerability indicators of the DCN, as well as a model that describes the vulnerability coefficient of the OBI network.

IV. Methods and models

To solve the problem of choosing between different OBI IS systems, it is necessary to consider a single dynamic coefficient of the IS threats occurrence [24]. This coefficient $P^{DT} \in [0;1]$ makes it possible to take into account the dynamics of IS threats, for example, for DCN OBI, as well as to model the likelihood of DCN threats.

As a rule, each organization or company that has been operating for some period of time already has certain statistics on information security incidents. And, therefore, one can talk about the statistical probability of the threats implementation $P_{stat} \in [0;1]$. One can also rely on expert assessments of DCN OBI threats $P_{\text{expert}} \in [0;1]$.

In a number of works, for example, [24], [25], [26], it was proposed to take into account the dynamic component of threats ($DC \in [0;1]$) of DCN IS:

$$DC = \begin{cases} P_{stat}^{n-1} > P_{stat}^{n}, & \left(\frac{P_{stat}^{n-1} - P_{stat}^{n}}{P_{stat}^{n}} \right); \\ P_{stat}^{n-1} \le P_{stat}^{n}, & \left(-\frac{P_{stat}^{n-1} - P_{stat}^{n}}{P_{stat}^{n}} \right), \end{cases} \quad (1)$$

where $n-$ is statistical data on IS threats, for example, for DCN OBI. Data can be received, for example, as a result of monitoring information security events using SIEM, or based on IPS / IDS operation data.

Next, one should determine the protection elements of the DCN OBI. At this stage, for example, with the help of an expert, one can build histograms of vulnerabilities and threats for DCN. Figure 1 shows an example of such a histogram for the DCN.

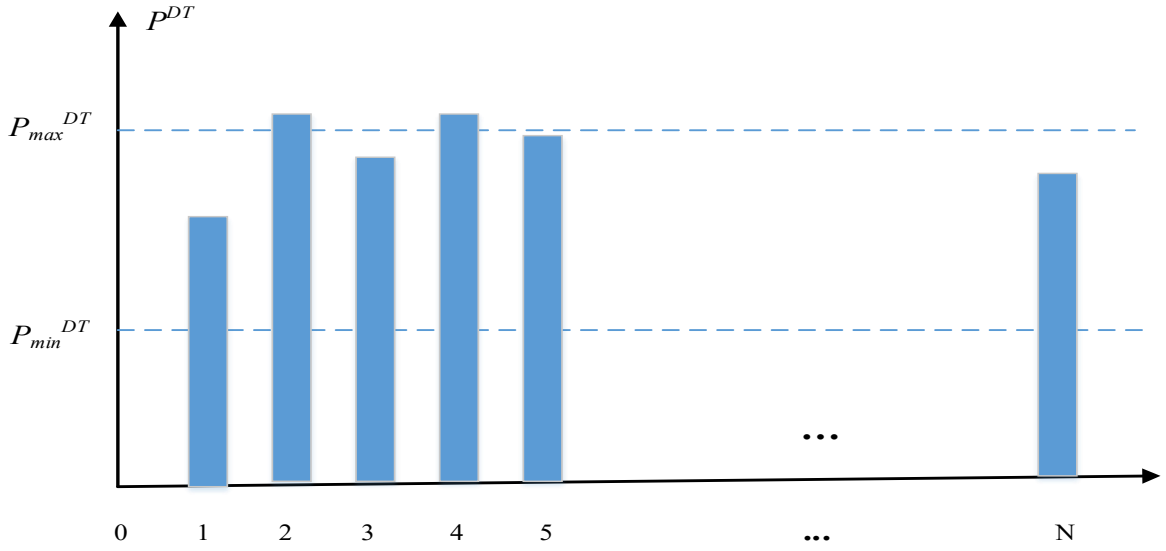

Fig. 1. Histogram with expert assessment of the significance of threats for the analyzed DCN

In Figure 1, the following numbering of threats caused by attacks is adopted (as an example, the DCN of an educational institution was considered):

1- remote attacks on the DCN infrastructure;

2 - remote attacks on telecommunications services or DCN servers;

3 - attacks after requests from the attacked DCN objects;

4 - attacks after the occurrence of the expected events at the attacked DCN object;

5 - unconditional attacks on the DCN.

N - other.

In cases when the threat occurs, the defense side faces an emergency. This situation requires considering all possible consequences of the threats implementation. For example, due to moral, material, informational losses, etc. for OBI.

Figure 1 shows that there is a maximum value of the threat realization probability $P_{\max}^{DT}$ and a minimum value of $P_{\min}^{DT}$. It can be interpreted like following:

If $P_n^{DT} > P_{\max}^{DT}$, then threat P_n^{DT} for example, for the DCN OBI, is accepted for a deeper analysis. It is automatically assigned to a high priority and measures are taken to prevent it;

If $P_{\min}^{DT} > P_n^{DT} > P_{\max}^{DT}$, then the given threat P_n^{DT} has medium priority;

If $P_n^{DT} > P_{\min}^{DT}$, then this threat P_n^{DT} is characterized by a low priority.

Therefore, at the first stage of analysis and assessment of threats it becomes possible for the employees of the information security department of the OBI to filter threats, for example, with the existing composition of the DCN information security system.

Next, consider the DCN vulnerability coefficient.

Vulnerability refers to the property of a WAN security element, such as a firewall, to be exposed to a threat. It states that ISS can be influenced by destabilizing factors. As the simplest destabilizing factor range affecting the firewall, we can separately consider:

- access to the DCN OBI of an untrusted application;
- access to DCN OBI using RAW Socket;
- the introduction of foreign DLLs into trusted processes of the DCN OBI;
- creation of Trojan streams in the trusted processes of DCN OBI;
- modification of the machine code of trusted processes;
- masking an untrusted process;
- and etc.

The DCN OBI vulnerability coefficient can be interpreted as a quantitative assessment of the information security level at the current time. Moreover, such an assessment is associated with the specific conditions for the functioning of the DCN and the OBI as a whole. The approach to the formation of the DCN vulnerability coefficient (or OBI in general) is shown in Figure 2.

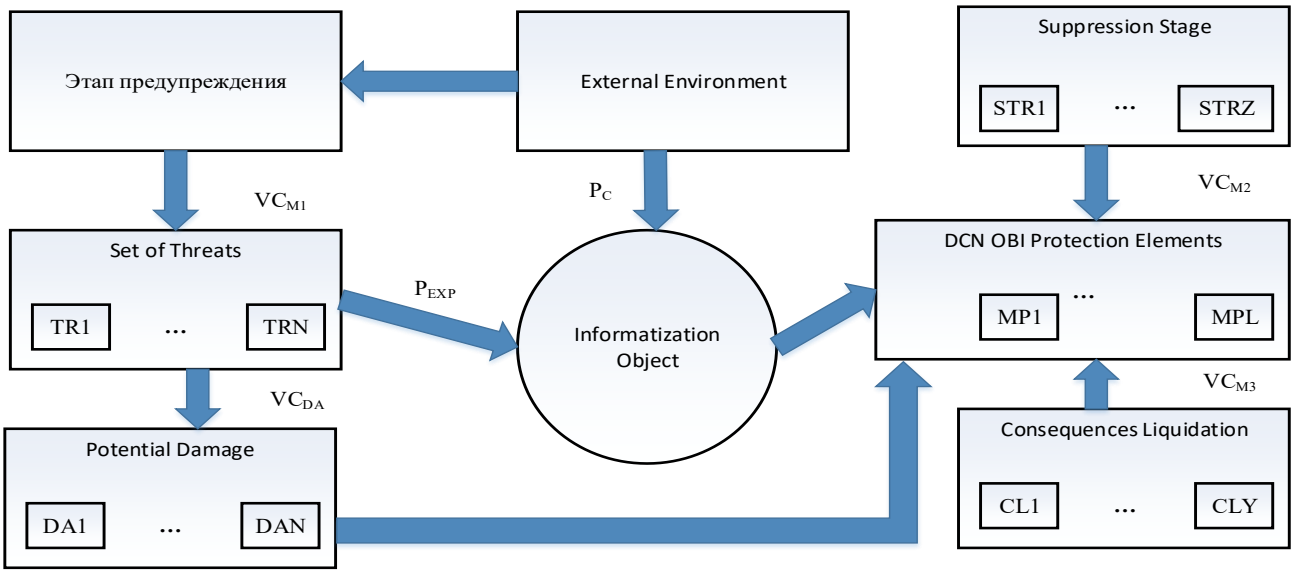

Fig. 2. Approach to the formation of the vulnerability coefficient of the DCN (or OBI as a whole)

Taking into account the results of work [24-26] the value of the vulnerability coefficient (VC) DCN can be represented as following:

$$VC = \sum_{i=1}^{N} VC_i \cdot \frac{\sum_{j}^{M} DC_{ij}}{\max \sum_{j}^{M} DC_{ij}}, \quad (2)$$

where $VC_i -$ is the value of the vulnerability coefficient for the $i-$th DCN IS threat; $DC_{ij} -$ the value of the damage coefficient for the $j-$th component of the DCN (for example, IS tools) with the $i-$th threat to IS; $N -$ the number of threats to DCN IS; $M -$ the number of DCN elements, including the information protection system.

Only organizational measures are usually not enough to eliminate threats. Effective protection, as a rule, requires financial investments for the purchase of information protection technical means, staff training and additional involvement of highly qualified specialists.

To solve the problem of the number of information security facilities determination, their technical parameters based on integrated information security metrics, for the DCN OBI, the annual reduced costs are taken as the target function:

$$C = p \cdot \sum_{i=1}^{n} CE_i + \sum_{i=1}^{m} OC_i, \quad (3)$$

where $p -$ is the coefficient that characterizes the comparative efficiency of capital investments in DCN IS for the analyzed OBI, CE_i, $OC_i -$ respectively, the i-th item of capital and operational costs for DCN IS; $n, m -$ the number of components of capital and operating costs for IS DCN, respectively.

To simplify the model, it was assumed that the annual reduced costs of DCN IS is the main criterion for the effectiveness of investing in the DCN IS system evaluation. Such simplification demonstrates the overall performance of the model. The simplicity of the calculation formula for the objective function (OF) makes it possible to simplify the analysis of the results for the adequacy of the model for solving the problem of determining the optimal composition of the information security system for DCN.

The costs of acquiring specific information security tools (within a specific class of threats, for example, firewall, IPS / IDS, SIEM, etc.) for IS RCS, represent a function:

$$CE_{1u} = a_1 + a_2 \cdot IPI, \quad (4)$$

where $IPI -$ is the integral performance indicator ISS of a certain class (for example, a firewall, IPS / IDS, SIEM, etc.); $a_1, a_2 -$ linear approximation coefficients.

Similarly, it is possible to express the capital costs associated with the acquisition of other information security classes for DCN (for example, access control), installation, and connection, for example, to the OBI information system.

Operating costs and constraints can be expressed using a similar approach. Although, as it was shown in [27-30], the approximation expressions are not necessarily linear.

In the proposed methodology, it was introduce a set CR of key partial criteria that is necessary to detail the description of the IS system for DCN (or OBI):

$$CR = \{CR_1, CR_2, CR_3, CR_4, CR_5\}, \quad (5)$$

where $CR_1 -$ is the cost of information security related to a certain class; $CR_2 -$ the number of classes of threats for the OBI information security, which will be blocked by the corresponding information security facilities; $CR_3 -$ the size of the leveled risk, which is reduced due to one or another class of information security for DCN; $CR_4 -$ availability of IS certificates for the relevant information security facilities; $CR_5 -$ indicator of compatibility of a separate information security facility in the general complex of protection and information security of the OBI.

Each of the private criteria specified above can vary in the range from 0 to 1. For example, for CR_5, if a particular information security facility is compatible with the rest in the group of facilities located on the protected DCN node, then the value is $CR_5 = 1$ (otherwise $CR_5 = 0$). For the criterion CR_1, the interpretation can be as follows:

$$CR_1 = \begin{cases} 1, & if \quad C_{ist} < C_{ist}^{\max}; \\ 0{,}5 & if \quad 0{,}5 \cdot C_{ist}^{\max} \le C_{ist} \le C_{ist}^{\max}; \\ 0 & if \quad C_{ist} > C_{ist}^{\max}, \end{cases} \tag{6}$$

where $C_{ist}, C_{ist}^{\max}$ – is the average cost of the information security system within the analyzed class (for example, firewalls, access control tools, intrusion detection systems, etc.) and the maximum cost.

For the criterion, the interpretation can be as following [27]:

$$CR_2 = \begin{cases} 1, & if \quad \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} = |IST|; \\ 0{,}5 & if \quad 0{,}5 \cdot |IST| \le \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} \le |IST|; \\ 0{,}25 & if \quad 0 < \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} \le 0{,}5 \cdot |IST|; \\ 0 & if \quad \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} = 0, \end{cases} \tag{7}$$

where $IST-$ is the set of DCN IS threats (the value is not constant and depends on external factors); $n-$ the number of actual threats for a particular DCN; $m_{ISR_{ii}}^{ist_k}$ – matrix of overlapping actual cyber threats, existing and planned means of protection and information security of the DCN.

For the criterion CR_3, , the interpretation can be as following [27]:

$$CR_3 = \begin{cases} 1, & if \quad \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} < R_a; \\ 0{,}5 & if \quad R_a \le \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} \le 0{,}5 \cdot R_{cr}; \\ 0{,}25 & if \quad 0{,}5 \cdot R_{cr} \le \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} \le R_{cr}; \\ 0 & if \quad \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} \ge R_{cr}, \end{cases} \tag{8}$$

where $R_a, R_{cr}-$ respectively, are the acceptable and critical levels of IS risk for DCN OBI; $n-$ the number of actual threats for a particular DCN; $m_{ISR_{ii}}^{ist_k}$ – a matrix of overlapping actual threats to information security, existing and planned information security facilities.

Similar calculations for partial criteria are repeatedly described in the scientific literature, for example, [10], [12], [16], [21].

Then, using the proposed particular criteria, it is possible to represent the efficiency (EF) of the entire IS system for DCN as a vector of the form:

$$EF = \{1, 1, 1, 1, 1\}. \tag{9}$$

Actually, in such a form, one can get the reference private criteria used to evaluate the effectiveness of the information security system for DCN.

Then, taking into account the above, one can represent the DCN vulnerability coefficient as following:

$$VC = \sum_{j=1}^{M} \frac{EF\left[P_{\text{expert (i)}} \cdot \left(P_{stat\,(i)} + DC_i\right)\right]}{\sum_{j}^{M} \alpha_{ij} \cdot CEF_{ij}}, \tag{10}$$

where $\alpha_{ij}-$ are the values of the weight coefficients that characterize the degree of influence of the th DCN IS tool at the corresponding stages of blocking the $j-$ th threat for the DCN IS; $CEF_{ij}-$ values of weight coefficients that characterize the effectiveness of the IS DCN IS tools (for example, firewall, IPS/IDS, SIEM, etc.) at the corresponding stages of blocking the $i-$ th DCN IS threat.

Thus, having, for example, simulation results, it is possible to analyze the components of the RCS vulnerability coefficient and choose a more effective set of information security tools to protect against attacks.

V. Experimental Studies of the Methodology for the Formation of an Integrated IS OBI System

A virtual network of conditional OBI has been designed for experimental verification of the effectiveness of the proposed methodology for the formation of the OBI IS system. VmWare Workstation platform installed on a computer running Windows 10 was used. The computer itself is based on the Intel Xeon E5 1650 server processor and has 32 GB of RAM installed, which is enough for virtual machine (VM) creation and system simulation operations.

A total of 3 virtual machines were created, 2 of which are running Proxmox VE OS, which acts as a hypervisor for deploying other VMs on it. The third VM was running the Ubuntu Server operating system. Also installed on this VM is the EVE-NG network modeling application.

For more convenient infrastructure management, cluster solutions were used. Such an approach made it possible to combine several servers into one system, which provided resource reservation and centralized administration. Since Proxmox VE also supports this feature, it was decided to combine 2 servers into one cluster. After the cluster has been created, by going to the address of any of the hosts, one can see information about both servers and all their resources (VMs, containers, storages, etc.). (Figure 3.)

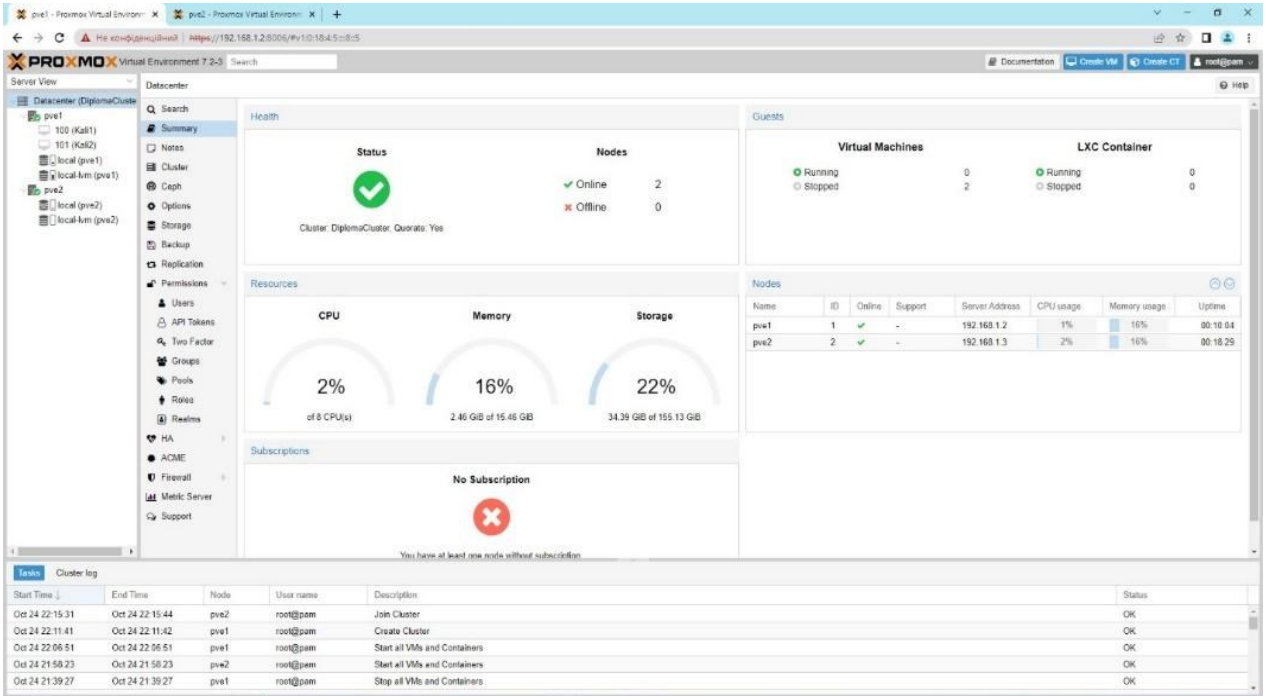

Fig. 3. Information about cluster resources

The creation of a cluster provides a large number of benefits. One of which is the ability to migrate VMs contained on servers to other cluster nodes.

As mentioned above, the EVE-NG application was used to create the OBI network model on network devices. 1 router (acting as a firewall) and 2 core switches were added. The first is responsible for the server segment, and the second for the user segment. Access switches were also added, connected to the core switch responsible for the user segment. There are 2 groups in the user segment: 1 - switches located in the premises of the OBI personnel, 2 - located on the premises where the OBI management works. Accordingly, it was accepted that the access policy for users from these 2 segments is different - users connected through management switches have more access rights to local resources located on the OBI servers, see fig. four.

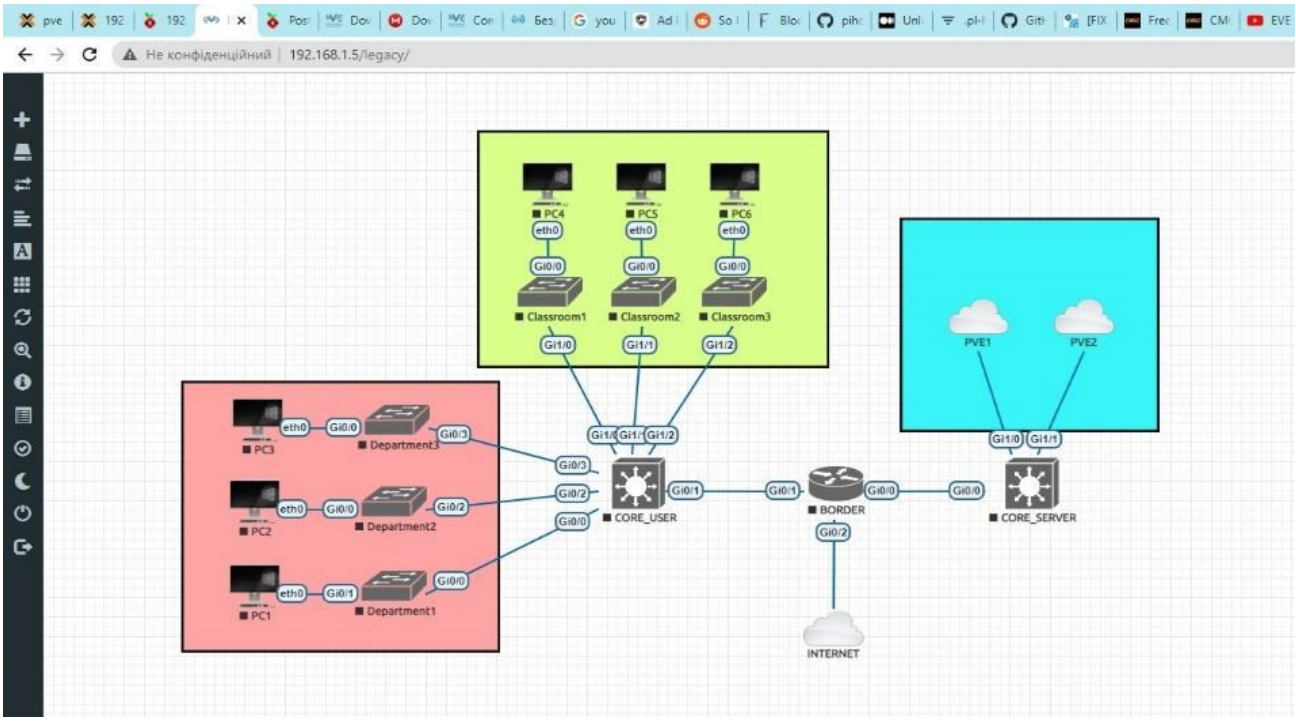

Fig. 4. Scheme of the OBI network

All devices connect to VmWare virtual interfaces. The VmWare interfaces, in turn, are connected to the network interface of the personal computer. The PC itself was connected to a router that is already connected to the ISP's network.

As part of the study of the methodology for the formation of an integrated OBI information security system, it was decided to change the settings of the OBI network in such a way as to make it more secure against external attacks. It was decided to redundant the core switches and their connections between themselves and the router. To do this, connections must be made from the servers and user access switches to both core switches. Most access switches, today, have 2-4 upstream ports for this, as well as servers - network cards with at least 2 ports, see Fig. 5.

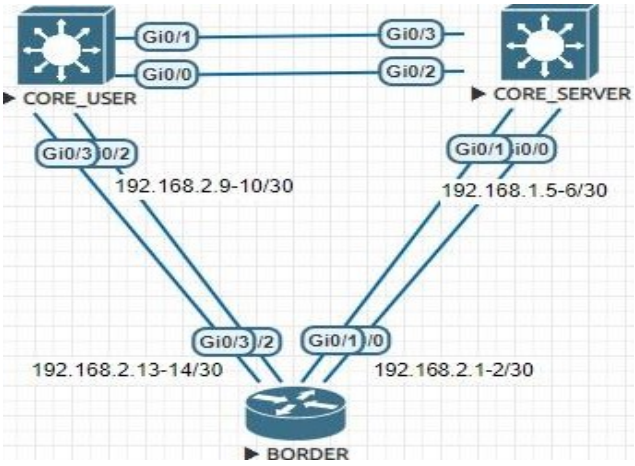

Fig. 5. Ensuring fault tolerance of OBI network switches

For communication between the router and the core switches, a dynamic routing protocol supported by most manufacturers - OSPF was configured, see Fig. 6.

```
**************************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**************************************************************************
BORDER>en
BORDER#conf t-
          ^
% Invalid input detected at '^' marker.

BORDER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BORDER(config)#router ospf 1
BORDER(config-router)#router-id 2.2.2.2
BORDER(config-router)#network 192.168.2.1 0.0.0.3 area 0
BORDER(config-router)#network 192.168.2.5 0.0.0.3 area 0
BORDER(config-router)#network 192.168.2.10 0.0.0.3 area 0
BORDER(config-router)#network 192.168.2.14 0.0.0.3 area 0
BORDER(config-router)#exit
BORDER(config)#router ospf 1
BORDER(config-router)#router-id 1.1.1.1
BORDER(config-router)#network 192.168.2.1 0.0.0.3 area 0
BORDER(config-router)#network 192.168.2.5 0.0.0.3 area 0
BORDER(config-router)#network 192.168.2.10 0.0.0.3 area 0
BORDER(config-router)#network 192.168.2.14 0.0.0.3 area 0
BORDER(config-router)#defaul-information originate
                     ^
% Invalid input detected at '^' marker.

BORDER(config-router)#default-information originate
BORDER(config-router)#exit
BORDER(config)#exit
BORDER#co
*Nov  6 17:40:36.906: %SYS-5-CONFIG_I: Configured from console by consol
BORDER#copy run
BORDER#copy running-config star
BORDER#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BORDER#
*Nov  6 17:41:03.052: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Nov  6 17:41:03.940: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
BORDER#
```

Fig. 6. Configuring the OSPF protocol

Next, virtual networks (VLANs) were created on the core switches. This made it possible to divide traffic into subnets to provide information security for OBI resources, to which limited access should be provided. STP has also been configured on the switches to avoid network loops. In addition, DHCP snooping protocols, ARP packet inspections, and traffic filtering for flood attacks were configured.

In order to further strengthen the protection of the OBI network, in addition to ensuring security at its individual nodes and filtering DNS addresses, it is advisable to add a VM to the system that would analyze traffic to detect cyber attacks. We decided to create a separate VM based on Kali Linux (Debian) with IPS Suricata installed, see Fig. 7.

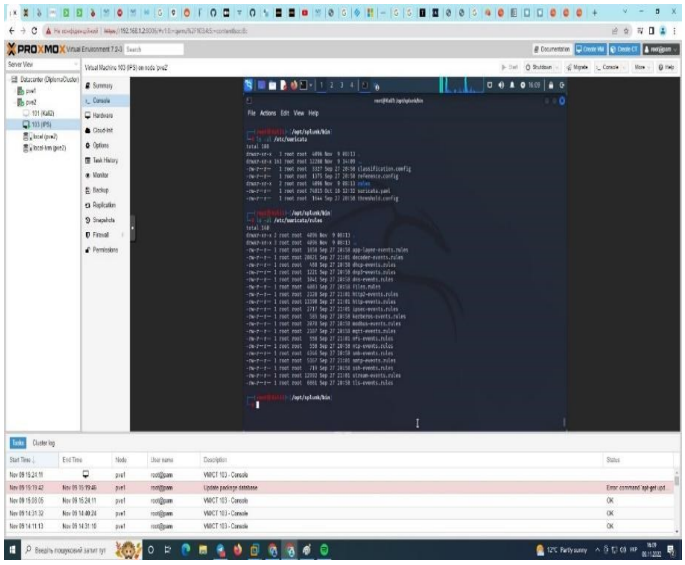

Fig. 7. Viewing IPS Suricata files

After completing the configuration of the secure OBI network, the performance was tested. To do this, the Pi-Hole VM was listed as the primary DNS server on all devices and on the edge router. The Pi-Hole app itself allowed a real-time view of which requests were blocked and which were allowed. With the help of Pi-Hole, it was convenient for the IS OBI administrator to display statistics in the form of charts and view their details.

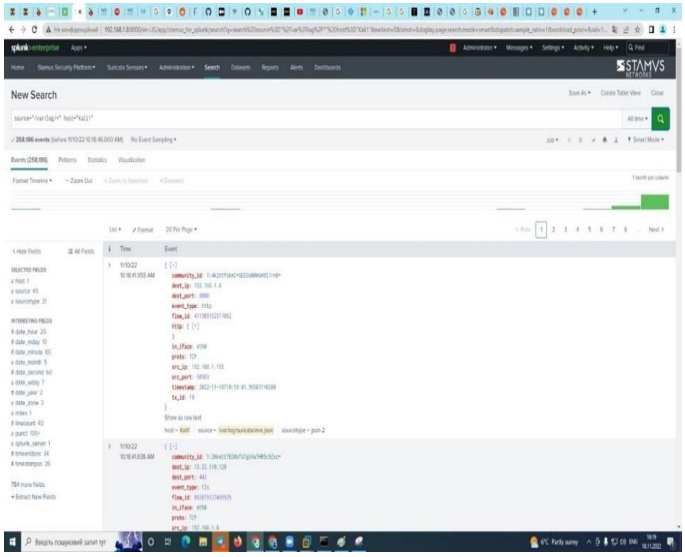

Fig.8. IDS Suricata system alerts

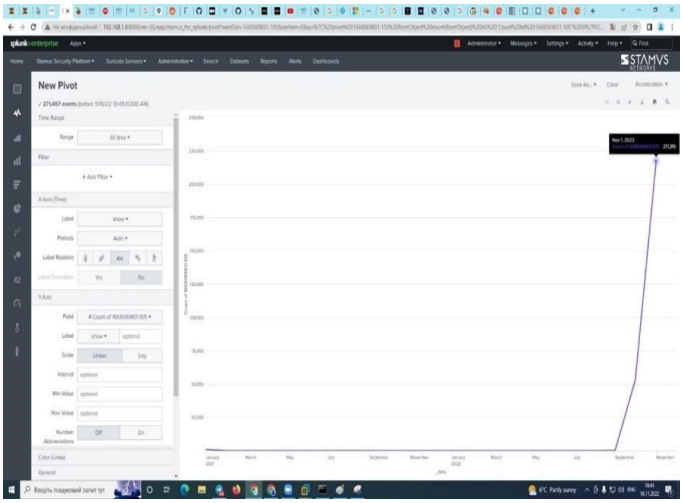

Fig.9. Graphical display in Splunk of alerts from IDS Suricata

VI. Discussion of Simulation Results

It can be seen from the obtained results, see fig. 8 and 9 that the tested IS system for virtual DCN (compiled on the basis of the proposed methodology) blocked more than 3700 malicious requests in 5 hours of operation, which is > 41% of all traffic entering the OBI network. Thus, the correctness of the decisions made on the use of IDS and SIEM systems to improve the information security of the OBI network was experimentally confirmed. After IDS Suricata and SIEM Splunk were configured, the latter began to receive system notifications from the former. In just an hour, 20 notifications were sent through the system about violations of OBI IS rules and blocking of the corresponding traffic. This led to the conclusion that such systems justify themselves in the OBI safety circuits.

It should be noted the possibility of this mathematical approach for assessing the level of IS not only for DCN, but for OBI as a whole. As a shortcoming of the study at the current stage, it can be indicated that an incomplete list of threats to the DCN or the OBI as a whole was considered. Also, during the experiment, the list of IS measures chosen to neutralize them was limited.

Conclusion

Thus, the conducted research allowed one to obtain the following results:

- A technique for the formation of an information security system for a distributed computer network (DCN) OBI is proposed.
- At the first stage of the methodology, it was proposed to use mathematical modeling based on the usage of the probability theory apparatus. The proposed approach made it possible to obtain an analytical expression for calculating the DCN vulnerability coefficient (if necessary, in general for the OBI).
- At the second stage of the methodology for the formation of the DCN IS system, methods of simulation modeling and virtualization of the IS components of the OBI network were used.
- In the course of experimental studies, a model of a secure OBI network has been built. In the experimental model, network devices and IS components were emulated on virtual machines (VMs). The resources of the OBI network were emulated by the server virtualization system Proxmox VE. The IPS Suricata threat detection system has been deployed on the hosts of the OBI network under PVE control, and the Splunk system was used as a SIEM.
- It is shown that the proposed method of forming the IS system for the DCN and the model of the vulnerability coefficient make it possible to obtain a quantitative assessment of the levels of vulnerability of various elements of the DCN. Also, the proposed model makes it possible, at the design stage of the network information security system, to assess the predicted level of vulnerability of the OBI and to carry out a preliminary assessment of the effectiveness of countermeasures to neutralize threats and vulnerabilities.

Acknowledgements

The work was carried out within the framework of the grant study AP08855887-OT-20 "Development of an intelligent decision support system in the process of investing in cyber security systems."

References

[1] Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. Computers & Security, 80, 74-89.

[2] Pérez-González, D., Preciado, S. T., & Solana-Gonzalez, P. (2019). Organizational practices as antecedents of the information security management performance: An empirical investigation. Information Technology & People, 32(5), 1262-1275. https://doi.org/10.1108/ITP-06-2018-0261

[3] Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: the security incident response perspective. IEEE Communications Surveys & Tutorials, 23(4), 2525-2556. https://doi.org/10.1109/COMST.2021.3117338

[4] 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. https://doi.org/10.1134/S1064230720020124

[5] Ahmetoglu, H., & Das, R. (2022). A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. Internet of Things, 100615. https://doi.org/10.1016/j.iot.2022.100615

[6] An, P., Wang, Z., & Zhang, C. (2022). Ensemble unsupervised autoencoders and Gaussian mixture model for cyberattack detection. Information Processing & Management, 59(2), 102844. https://doi.org/10.1016/j.ipm.2021.102844

[7] Aribisala, A., Khan, M. S., & Husari, G. (2021, October). Machine Learning Algorithms and Their Applications in Classifying Cyber-Attacks On a Smart Grid Network. In 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0063-0069). IEEE.

[8] Angelini, M., Blasilli, G., Catarci, T., Lenti, S., & Santucci, G. (2018). Vulnus: Visual vulnerability analysis for network security. IEEE transactions on visualization and computer graphics, 25(1), 183-192.

[9] Yeboah-Ofori A, Islam S. Cyber Security Threat Modeling for Supply Chain Organizational Environments. Future Internet. 2019; 11(3):63. https://doi.org/10.3390/fi11030063

[10] Tanwar, R., Choudhury, T., Zamani, M., & Gupta, S. (Eds.). (2020). Information Security and Optimization. CRC Press.

[11] Almohri, H. M., Watson, L. T., Yao, D., & Ou, X. (2015). Security optimization of dynamic networks with probabilistic graph modeling and linear programming. IEEE Transactions on Dependable and Secure Computing, 13(4), 474-487. https://doi.org/10.1109/TDSC.2015.2411264

[12] Bouyeddou, B., Harrou, F., Kadri, B., & Sun, Y. (2021). Detecting network cyber-attacks using an integrated statistical approach. Cluster Computing, 24(2), 1435-1453. https://doi.org/10.1007/s10586-020-03203-1

[13] Utzerath, J., & Dennis, R. (2021). Numbers and statistics: data and cyber breaches under the General Data Protection Regulation. International Cybersecurity Law Review, 2(2), 339-348. https://doi.org/10.1365/s43439-021-00041-8

[14] Schatz D., Bashroush R. Economic valuation for information security investment: a systematic literature review //Information Systems Frontiers. – 2017. – Т. 19. – №. 5. – С. 1205-1228. (2017) https://doi.org/10.1007/s10796-016-9648-8

[15] Gordon L. A. et al. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities //Journal of Accounting and Public Policy. – 2006. – Т. 25. – №. 5. – С. 503-530. (2006) https://doi.org/10.1016/j.jaccpubpol.2006.07.005

[16] Gordon L. A., Loeb M. P., Lucyshyn W. Sharing information on computer systems security: An economic analysis //Journal of Accounting and Public Policy. – 2003. – Т. 22. – №. 6. – С. 461-485. (2003) https://doi.org/10.1016/j.jaccpubpol.2003.09.001

[17] Qin W., Jianming Z. H. U. Research on the game of information security investment based on the Gordon-Loeb model //Journal on Communications. – 2018. – Т. 39. – №. 2. – С. 174. (2018) https://doi.org\10.11959/j.issn.1000-436x.2018027

[18] David, D. P., Mermoud, A., & Gillard, S. (2021). Cyber-Security Investment in the Context of Disruptive Technologies: Extension of the Gordon-Loeb Model. arXiv preprint arXiv:2112.04310

[19] Averyanova, Y., Sushchenko, O., Ostroumov, I., Kuzmenko, N., Zaliskyi, M., Solomentsev, O., ... & Tserne, E. (2021). UAS cyber security hazards analysis and approach to qualitative assessment. In Data Science and Security (pp. 258-265). Springer, Singapore.

[20] Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. Computers & Security, 103, https://doi.org/10.1016/j.cose.2021.102196

[21] Deb, R., & Roy, S. (2021). A Software Defined Network information security risk assessment based on Pythagorean fuzzy sets. Expert Systems with Applications, 183, https://doi.org/10.1016/j.eswa.2021.115383

[22] Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. Software and Systems Modeling, 21(1), 157-177.

[23] Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

[24] George, P. G., & Renjith, V. R. (2021). Evolution of safety and security risk assessment methodologies towards the use of bayesian networks in process industries. Process Safety and Environmental Protection, 149, 758-775.

[25] Koz'minyh, S. I. (2018). Matematicheskoe modelirovanie obespecheniya kompleksnoj bezopasnosti ob"ektov informatizacii kreditno-finansovoj sfery. Voprosy kiberbezopasnosti, (1 (25)), 54-63.

[26] Lakhno, V., Akhmetov, B., Smirnov, O., Chubaievskyi, V., Khorolska, K., Bebeshko, B. Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm (2023) Lecture Notes on Data Engineering and Communications Technologies, 131, pp. 21-34.

[27] Lakhno, V., Akhmetov, B., Mohylnyi, H., Blozva, A., Chubaievskyi, V., Kryvoruchko, O., Desiatko, A. Multi-criterial optimization composition of cyber security circuits based on genetic algorithm (2022) Journal of Theoretical and Applied Information Technology, 100 (7), pp. 1996-2006.

[28] Olad'ko V.S. Model' vybora racional'nogo sostava sredstv zashchity v sisteme elektronnoj kommercii // Voprosy kiberbezopasnosti. 2016. № 1. S. 17–23.

[29] Prokushev, YA. E., Ponomarenko, S. V., & Ponomarenko, S. A. (2021). Modelirovanie processov proektirovaniya sistem zashchity informacii v gosudarstvennyh informacionnyh sistemah. Computational nanotechnology, (1), 26-37.

[30] Lakhno, V., Mazaraki, A., Kasatkin, D., Kryvoruchko, O., Khorolska, K., Chubaievskyi, V. (2023). Models and Algorithms for Optimization of the Backup Equipment for the Intelligent Automated Control System Smart City. In: Ranganathan, G., Fernando, X., Rocha, Á. (eds) Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems, vol 383. Springer, Singapore. https://doi.org/10.1007/978-981-19-4960-9_57