СЕКЦИЯ 2. ТЕХНОЛОГИЯ

УДК: 004.056.52 DOI: 10.47813/nto.2.2022.5.78-87 EDN: MWDADK

Формализация метода реализации защищенного обмена данными на основе динамической топологии сети

Е.А. Кушко*, Н.Ю. Паротькин

Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, просп. им. газ. «Красноярский рабочий», 31, Красноярск, 660037, Россия

*E-mail: evgeny.kushko@gmail.com

Аннотация. Автором предложено решение по защите от исследования внутрисетевого обмена от стороннего наблюдателя. Данное решение построено на принципах лавинной маршрутизации, группового вещания и технологии движущейся цели. Метод отличается от существующих подходом к коммутации и обмена данными, позволяющий скрыть стороны межсетевого обмена, что значительно затрудняет анализ сетевого трафика. В работе приведено формализованное описание разработанного метода, его аналитическая модель и результаты моделирования узла-ретранслятора. Данный метод применен в качестве меры повышения уровня защищенности сенсорной сети.

Ключевые слова: безопасность локальной сети, защита сети от исследования, защищенный обмен данными, технология движущейся цели

Formalization of secure data communication implementation method based on dynamic network topology

E.A. Kushko*, N.Yu. Parotkin

Reshetnev Siberian State University of Science and Technology, Krasnoyarskii rabochii pr., 31, Krasnoyarsk, 660037, Russia

*E-mail: evgeny.kushko@gmail.com

Abstract. In this study the author proposes a solution for countering research of network traffic by an outside observer. The proposed solution is based on avalanche routing, group broadcasting and moving target technology. This method differs from the existing solutions by switching and data exchange approach: the developed approach allows to hide participants of the network interaction; thus, network traffic analysis is significantly hindered. The paper presents a formalized description of the developed method, its analytical model and simulation results of the repeater node. This method is used to increase the sensor network security level.

Keywords: local area network security, network scanning protection, secure data transfer, moving target defense

1. Introduction

According to Positive Technologies, Infowatch and other large companies' analytics, enterprise networks are vulnerable and an attacker can penetrate them. It is also emphasized that detecting an intruder after penetration is quite difficult. Typically, after penetration the intruder carries out network traffic research [1]. The attacker has almost unlimited amount of time and can accurately plan his actions. Network topology and information systems characteristics are of increasing interest to intruders [2], because this data is essential for planning further attacks.

The proposed solution does not restrict the actions of the attacker, it only hinders network traffic analysis. As a result, the intruder cannot evolve the attack, because he has no information to plan it.

Sensor network is the lower layer of the Internet of Things. The sensor network is a dynamic, self-organizing, distributed network of sensors and execution units. It is designed to accomplish automation, diagnostics, telemetry and machine-to-machine interaction tasks. The following requirements are considered when building a sensor network: ease of deployment and operation, no need for frequent maintenance, high fault tolerance and reliability, scalability.

Internet of Things systems are essentially production and engineering process control systems; therefore, it is necessary to comply with FSTEC of Russia regulation №31 when building a security system. If the security system is designed for critical information infrastructure facility, it should comply with FSTEC of Russia regulation №239. These regulations require comprehensive technical approach to network security: building layered protection at all levels of the information system as well as hiding the architecture and configuration of the information system as an optional measure.

Generally, sensor network protection mechanisms are primarily aimed at ensuring high availability: providing stable communication channels, building optimal data transfer routes, protecting against denial-of-service attacks, etc. Tasks that a sensor network solves usually require high reliability, autonomy, and fault tolerance.

Sensor network devices should function for years in difficult industrial conditions, so data size, transfer range, power consumption and costs are limited. Consequently, these devices have low performance and operate in low bandwidth conditions [3].

The lack of intrusion detection, authentication and encryption mechanisms affects the security of sensor networks. Due to the low performance of devices, the mechanisms are usually greatly simplified, which makes them vulnerable.

Given all of the above factors, an attacker can penetrate the sensor network at minimal cost [4, 5]. In addition, an attacker can act from outside the controlled area, therefore, the use of this improving sensor network security method is justified.

2. Method description

The developed method of secure data communication for dynamic network topology is based on moving target technology [6]. Nodes participating in secure data communication move in transfer slots and transmit data using group broadcasting. Each node is simultaneously in multiple transfer slots, it redirects received data to all the slots it is connected at the moment, i.e., avalanche routing is used.

Early works [7, 8] describe the implementation of this method based on Wi-Fi, UDP Protocol and multicast groups, but an approbation of this early method as a sensor network protection measure showed that the choice of these technologies is not the best solution. For sensor networks, it is preferable to use such technologies as ZigBee or Z-Wave [9], as they have a mesh topology, higher power efficiency and range. Therefore, the further description of the method has been revised without specifying any communication technology, in order to find the optimal practical solution.

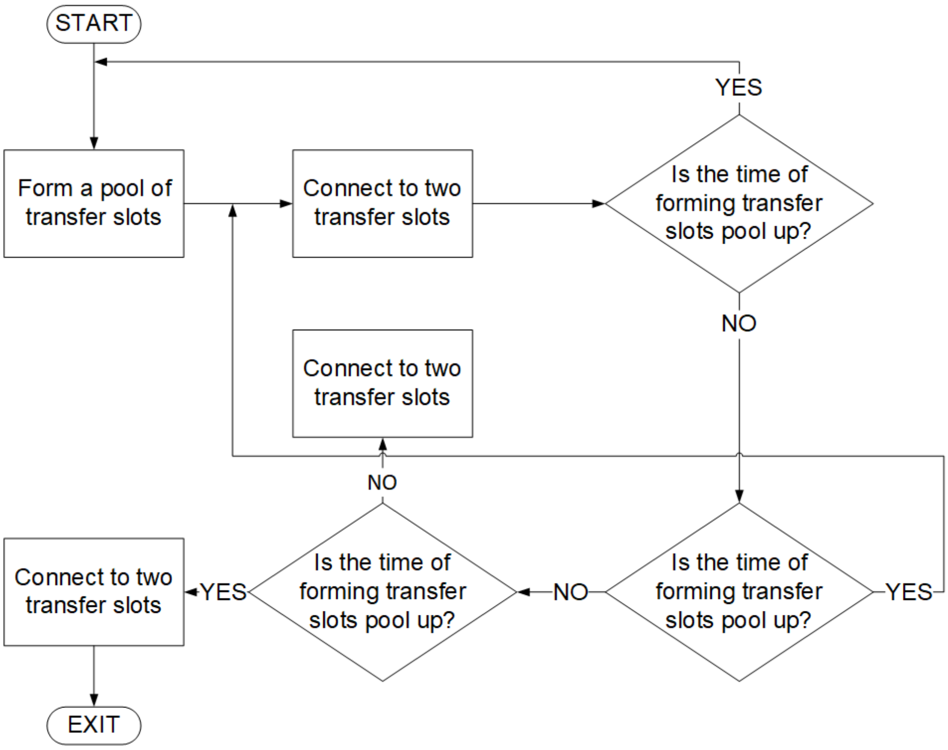
START
YES
Form a pool of transfer slots
Connect to two transfer slots
Is the time of forming transfer slots pool up?
NO
Connect to two transfer slots
NO
Connect to two transfer slots
YES
Is the time of forming transfer slots pool up?
NO
Is the time of forming transfer slots pool up?
YES
EXIT

Figure 1. Secure data communication initialization algorithm.

At the stage of initialization, each participant node forms a pool of transfer slots numbers, through which the data is transmitted, according to an algorithm depending on the current date and time. This pool of slots changes at regular intervals. After the pool is formed, the node selects two transfer slots and connects to them. At the end of another time interval, which is less than the interval for re-forming the transfer slots numbers pool, the node again randomly selects the transfer slots. The general algorithm for initializing secure data communication is shown in figure 1.

In order to transmit data, each node participating in secure data communication generates a data packet and transmits it to all currently connected transfer slots. All data packets are of the same size, and if the size of transmitted data exceeds the size of the packet, the data is split into several packets. The packet containing the receiver and sender IDs is encrypted with the receiver's public key using an RSA-1024 algorithm. Data packet structure is shown in figure 2. Nodes connected to receiving transfer slots retransmit the packet to all other transfer slots until every transfer slot gets the packet.

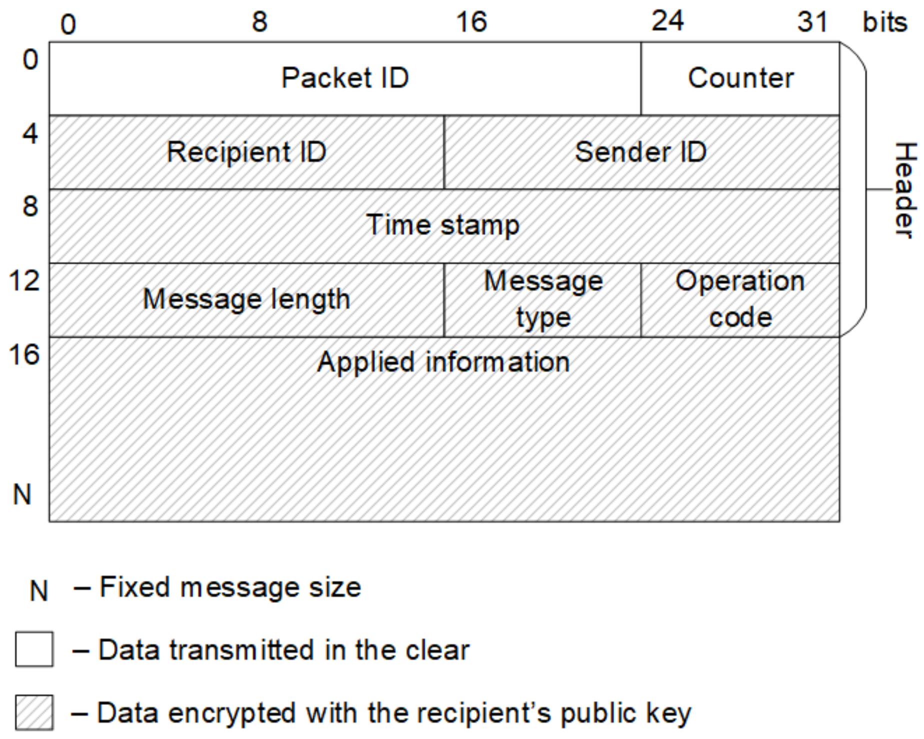

Figure 2. Data packet structure.

If the node with ID 3 intends to send data to the node with ID 5, then the node with ID 3 generates data packet where it specifies the node with ID 5 as a recipient, and itself as the sender. Next, node with ID 3 sends the data packet to all transfer slots it is connected (figure 3a).

In turn, each node of the receiving transfer slot, relay the packet to other active transfer slots where the node participates (figure 3b).

Each member node selects transfer slots in such a way as to have at least one common transfer slot with at least one other node that is a member of the secure data communication. In addition, data transfer by handshaking is provided. As a result, the data transfer between the sender and the recipient is guaranteed.

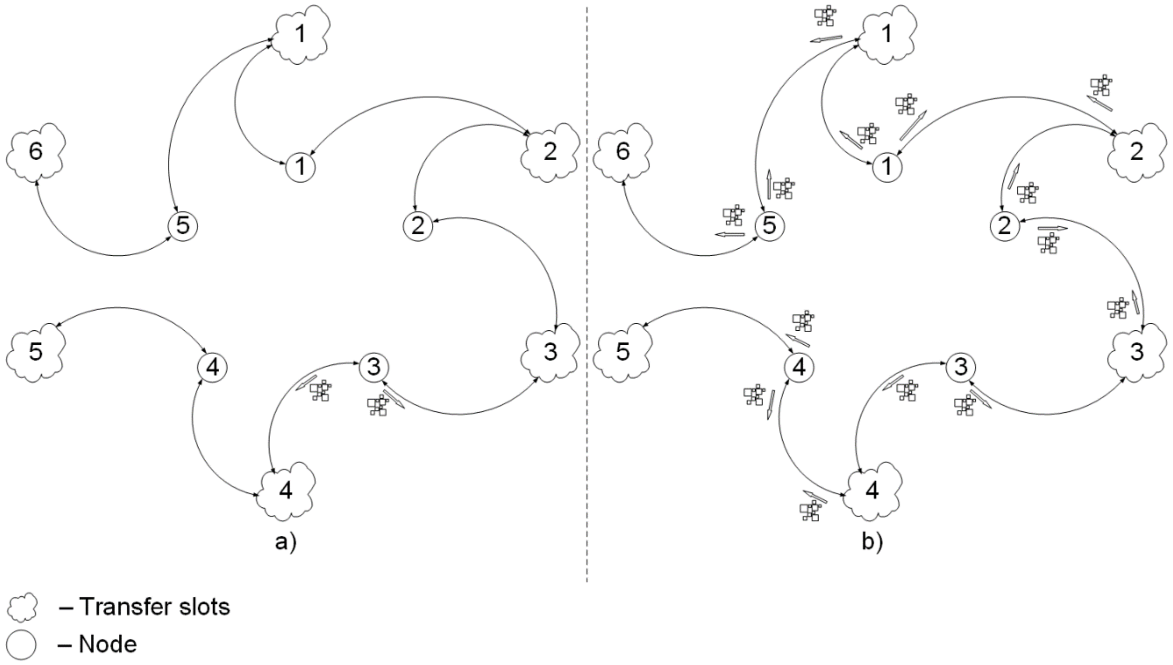

Figure 3. Data transfer: a) at the initial stage b) at the final stage.

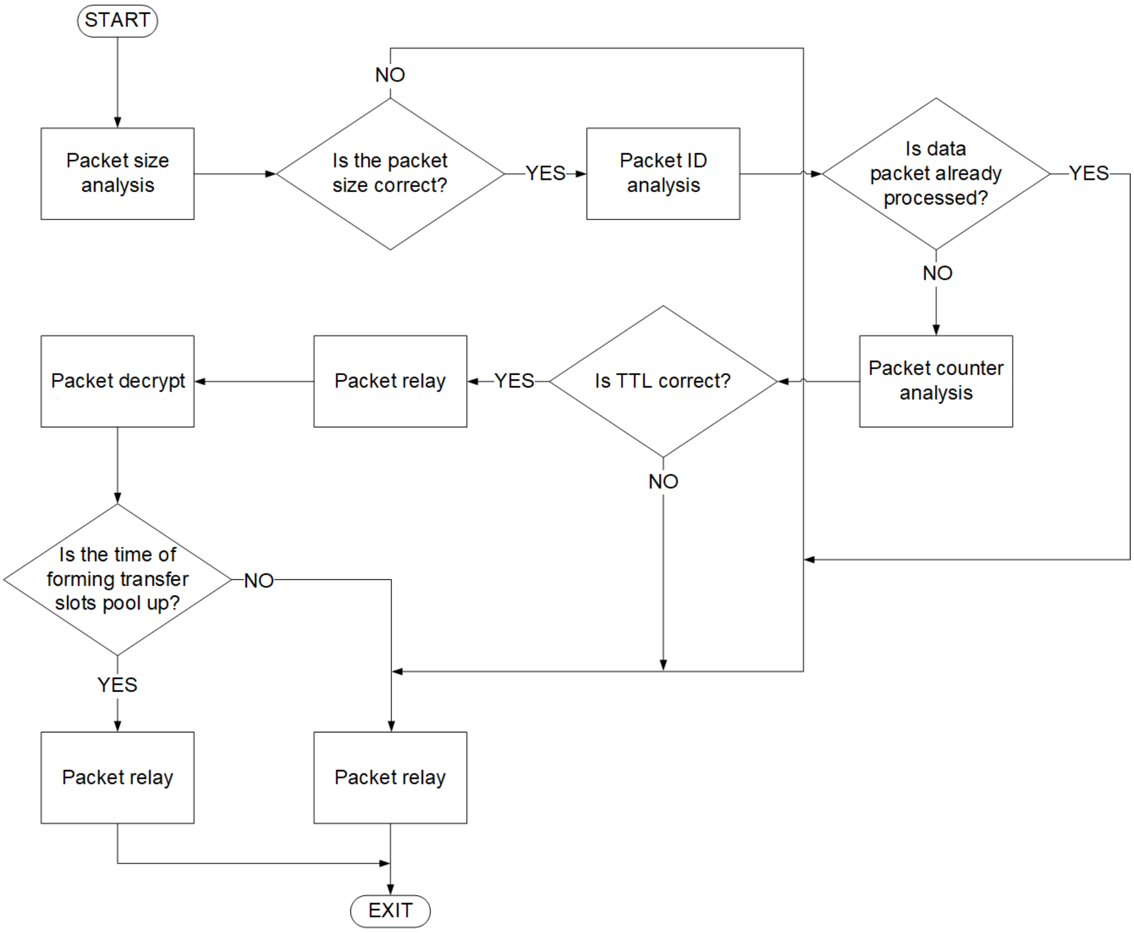

Figure 4. Incoming data packet processing algorithm.

After relaying, each node attempts to decrypt the packet and extract the corresponding identifier from its header. If the packet is successfully decrypted, the node processes it, otherwise the packet is discarded. Figure 4 shows the incoming data packet processing algorithm. To ensure that the relay is not infinite, each packet has a lifetime. After each retransmission, the node that relays the packet increments the packet counter; when the counter reaches the limit, the packet is not retransmitted anymore. Furthermore, the data packet is discarded if the maximum packet size is exceeded or the packet has been previously processed by another node whether it was meant for it or not.

When data is transmitted this way, an attacker who intercepts and analyses the data cannot identify receivers or senders, since the data packets do not explicitly contain their addresses. The data packet, regardless of the amount of data transmitted, has a fixed size and is encrypted. Furthermore, participants of the secure data communication switch between transfer slots and the logical structure of the system has a dynamic topology. Retransmission in combination with a fixed packet size does not allow to determine whether the packet is the request or response, and which node is the sender or receiver. As a result, an attacker cannot identify data flows or determine relationships between nodes, as well as cannot obtain long-term information about the logical structure of the system.

3. Analytical model

During the method approbation, occurred difficulties concerning method studying. Previous assessments and tests were carried out on a virtual or real infrastructure, which means difficulties in increasing data flows, and studying the network in whole, since the traffic was collected and analyzed on specific nodes. Therefore, it is necessary to develop an analytical model in order to use modeling tools to study the proposed method [10].

First of all, the model is needed to obtain network interaction statistics with taking into account processes occurring both on individual nodes and in the whole network.

Assuming that the speed between two neighboring nodes is constant, as the number of intermediate nodes in the transmission chain increases, the speed decreases.

Let us assume that packets arrive at the relay node according to the Poisson law [11] with some intensity λ (equation 1).

$$f(t) = \frac{(\lambda \mathrm{e})^n}{n!} e^{-\lambda t}, \tag{1}$$

where $f(t)$ – distribution density, λ – flow rate, n – number of traffic flows.

Incoming packets are queued for processing. The packet service time is the sum of the queue waiting time and the processing time. Processing includes searching for the packet ID in the list of previously processed ones, adding the packet ID in the list of previously processed and analysis of the counter to limit the relay. The counter analysis time can be neglected, since it is insignificant. The average packet service time T_{avg} is determined by the formula:

$$T_{avg} = T_w + T_h = p(k) + q(k) + g(\lambda n), \tag{2}$$

where T_w – queue waiting time, T_h – packet processing time, λ – flow rate, n – number of traffic flows, k – length of the list of previously processed packets IDs, $p(k)$ – linear time function searching an identifier in the list of previously processed, $q(k)$ – constant time function adding the packet ID in the list of previously processed, $g(\lambda n)$ – constant time function queuing incoming packets.

Depending on the purpose of the simulation, it may be necessary to take into account the data packets generating interval. For example, estimating the maximum bandwidth of such a network, it is necessary to choose a packet generation interval with negligible packet loss. As the intensity of data traffic increases, packet loss may also increase.

Since the network structure changes at certain time intervals, it is necessary to take into account the delays introduced by these mechanisms: the formation of transfer slots list, as well as disconnection and connection to them. Frame losses introduced by these mechanisms are offset by guaranteed handshake delivery.

4. Repeater node simulation

As an experiment, a simulation model of a repeater node in the GPSS environment was developed. Figure 5 shows the flowchart of the modeling process. During the simulation, the following parameters were estimated as the number of information flows passing through the node increased: utilization factor, average processing time, average request/response queue time, average requests/response queue length. The results are provided in the table 1.

Table 1. Simulation results.

Parameter \ Number of information flows	1	2	10	100	1000
Utilization factor	0.39	0.71	0.99	0.99	1
Average processing time (ms)	5.04	5.16	5.04	5.02	4.99
Average request queue time (ms)	21.60	24.79	98.59	1000.94	9981.04
Average response queue time (ms)	4.52	8.01	62.19	739.37	7473.35
Average requests queue length	0.83	1.71	9.68	99.7	999.7
Average response queue length	0.17	0.55	6.11	73.64	748.53

With an increase in the number of information flows passing through the repeater node, time characteristics of all parameters also increase. Since the method involves avalanche routing, all network nodes process the same number of information flows. The more repeater nodes are between the sending and the receiving nodes, the more decreases the bandwidth and increase the delays.

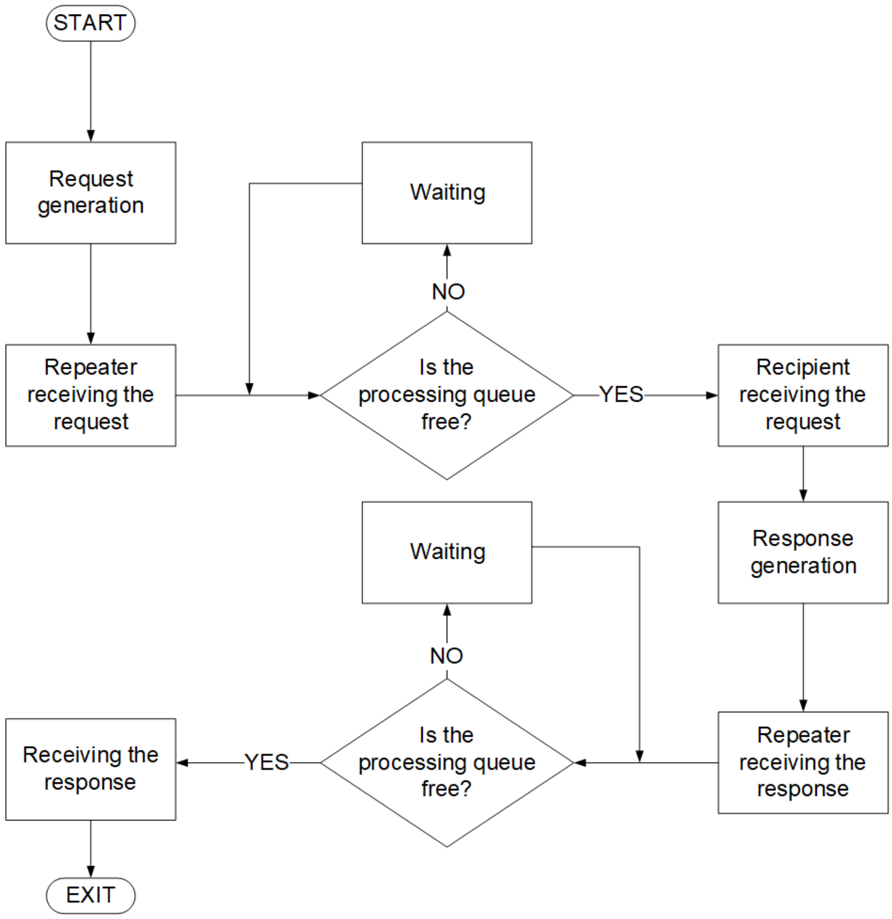
START
Request generation
Repeater receiving the request
Waiting
NO
Is the processing queue free?
YES
Recipient receiving the request
Response generation
Repeater receiving the response
Waiting
NO
Is the processing queue free?
YES
Receiving the response
EXIT

Figure 5. Flowchart of the modeling process.

If this method is used as a measure to increase the security level of the sensor network, the obtained performance characteristics are acceptable, since such networks generate a relatively small amount of network traffic. At the same time, for sensitive to delays systems, such a solution may not be applicable.

Further studies should aim at reducing the impact of multiple repeater nodes between the sending and receiving nodes on performance characteristics, considering implementation of this method on low-performance devices.

5. Conclusion

The paper provides a formalized description of secure data communication implementation method based on dynamic network topology without specifying particular technologies. The paper also describes an analytical model of this method. Based on this model and simulation tools, we conducted an experiment aimed at evaluating the performance characteristics of a repeater node and presented the results.

Acknowledgment

This work was supported by the Ministry of Digital Development, Communications and Mass Media of the Russian Federation for research project № 40469-07/2021-К (grant IS).

References

1. Positive Research 2020: website. – 2020. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2020-rus.pdf (date of visit: 31.05.2022)
2. Positive Research 2021: website. – 2021. – URL: https://www.ptsecurity.com/upload/corporate/ru- ru/analytics/positive-research-2021-rus.pdf (date of visit: 31.05.2022)
3. Rusanov, P. Wireless features touch networks / P. Rusanov, A. Yurochkin // The Bulletin of the Voronezh institute of high technologies. – 2019. – № 4(31). – P. 79-81.
4. Finogeev, A. G. Analysis and classification of attacks via wireless sensor networks in SCADA systems / A. G. Finogeev, I. S. Nefedova, E. A. Finogeev [et. al.] // Caspian Journal: Management and High Technologies. – 2014. – № 1. – P. 12-23.
5. Meleshko, A. Security analysis of software and hardware components in wireless sensor networks / A. Meleshko, V. Desnitsky // Telecom IT. – 2019. – V. 7. – P. 75-83.
6. Carvalho, M. Moving-Target Defenses for Computer Networks / M. Carvalho, R. Ford // IEEE Security and Privacy, Computer Society. – 2014. – V. 12. – P. 73-76.
7. Kushko, E. Method of hiding the architecture and configuration of the sensor network based on the dynamic topology / E. Kushko, N. Parotkin // IOP Conference Series: Materials Science and Engineering. – 2020. – №. 862.
8. Kushko, E. Concealment of sensor network node interaction / E. A. Kushko, N. Yu. Parotkin // IOP Conference Series: Materials Science and Engineering. – 2021. – № 1155.
9. Danbatta, S. Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation / S. Danbatta, A. Varol // 2019 7th International Symposium on Digital Forensics and Security (ISDFS). – 2019. – P. 1-5.
10. Popov, A. Implementation of a combined algorithm designed to increase the reliability of information systems: simulation modeling / A. Popov, V. Zolotarev, S. Bychkov // IOP Conference Series: Materials Science and Engineering. – 2016. – № 155.
11. Consul, P. A generalization of the Poisson distribution / P. Consul, G. Jain // Technometrics. – 1973. – V. 15. – № 4. – P. 791-799.