UDC 004.92
DOI: 10.31891/CSIT-2021-5-11

OLGA MOROZOVA, ARTEM TETSKYI,
National Aerospace University "Kharkiv Aviation Institute"
ANDRII NICHEPORUK, DENUS KRUVAK,
Khmelnytskyi National University
VITALII TKACHOV
Kharkiv National University of Radio Electronics

SMART HOME SYSTEM SECURITY RISK ASSESSMENT

The concept of the Internet of Things became the basis of the fourth industrial revolution, which allowed to transfer the processes of automation to a new saber. As a result, automation systems, such as smart homes, healthcare systems and car control systems, have become widespread. The developers of such systems primarily focus their efforts on the functional component, leaving safety issues in the background. However, when designing and operating IoT systems, it is equally important to assess potential bottlenecks and develop complete and comprehensive strategies to mitigate and eliminate the negative effects of cyberattacks.

The purpose of this study is to identify possible cyber threats and assess their impact on critical information objects in the smart home system. To achieve this goal, the three-level architecture of the smart home system is considered and a review of known cyber threats for each level is conducted. The critical information objects in the smart home system are the containers in which the information objects are stored, the risk assessment criteria and the cyber threat scenarios. The information security risks of the smart home system were assessed using the OCTAVE Allegro methodology for the information object that presents the information collected by the smart home sensors.

Keywords: security risk assessment, smart home, critical information object, threats

ОЛЬГА МОРОЗОВА, АРТЕМ ТЕЦЬКИЙ
Національний аерокосмічний університет ім. М.Є. Жуковського "Харківський авіаційний інститут"
АНДРІЙ НІЧЕПОРУК, ДЕНИС КРИВАК
Хмельницький національний університет
ВІТАЛІЙ ТКАЧОВ
Харківський національний університет радіоелектроніки

ОЦІНКА РИЗИКІВ БЕЗПЕКИ СИСТЕМИ РОЗУМНОГО БУДИНКУ

Концепція Інтернету речей стала основою четвертої промислової революції, що дозолило перевести на новий шабель процеси автоматизації. Наслідком цього стало широке поширення систем автоматизації зокрема, розумних будинків, систем у сфері охорони здоров'я та систем керування автомобілем. Розробники таких систем в першу чергу фокусують власні зусилля на функціональній складовій, залишаючи питання безпеки на другий план. Проте, при проектуванні та експлуатації систем Інтернету речей не менш важливим завданням є оцінка потенційних "вузьких" місць та розроблення повних та вичерпних стратегій по пом'якшенню та усуненню негативних впливів кібератак.

Метою даного дослідження є визначення можливих кіберзагроз та оцінка їх впливів на критичні інформаційні об'єкти в системі розумного будинку. Для досягнення мети у роботі розглянуто трьохрівневу архітектуру системи розумного будинку та проведено огляд відомих кіберзагроз для кожного рівня. Визначено критичні інформаційні об'єкти в системі розумного будинку контейнери, в яких зберігаються інформаційні об'єкти, критерії оцінки ризиків та сценарії кіберзагроз. Проведено оцінку ризиків інформаційної безпеки системи розумного будинку із залученням методології OCTAVE Allegro для інформаційного об'єкту, що представляє інформацію, зібрану датчиками розумного будинку. Проведений процес оцінки ризиків дозволяє проаналізувати інформаційні об'єкти в системі розумного будинку, які є критичними з точки зору безпеки, провести аналіз ризиків та їх впливів на об'єкти, та запропонувати можливі контрзаходи з метою захисту інформаційних об'єктів та створення системи розумного дому більш безпечним.

Перспективним напрямком подальших досліджень є формування комплексної оцінки ризиків інформаційної безпеки системи розумного будинку та реалізації програмної системи, що дозволить автоматизувати процес формування оцінки ризиків не тільки для системи розумного будинку, а й для інших систем, що імплементують принцип Інтернету речей.

Ключові слова: оцінка ризиків безпеки, розумний будинок, критичний інформаційний об'єкт, загрози.

Introduction

The growing popularity of the Internet of Things (IoT) provides ample opportunities to improve, plan and automate our lives. IoT allows you to network and manage multiple devices that provide data collection, analysis and transmission. The scope of IoT continues to expand every year, covering new areas of life, from smart homes, cities to healthcare.

However, along with the obvious benefits and conveniences of using IoT, the concept of the Internet of Things leaves a number of potential security bottlenecks for attackers. Users' personal data collected by smart devices is always of value to hackers and hijackers of confidential information. In addition, a cyberattack on an Internet of Things solution has the potential to damage physical services and physical infrastructure. When designing and operating Internet of Things systems, an important task is to assess these potential bottlenecks and develop complete and comprehensive strategies to mitigate and eliminate the negative effects of cyberattacks. Therefore, *the purpose of this study* is to identify possible cyber threats and assess their impact on critical information objects in the smart home system.

Three-level architecture of home automation systems and attacks on its components

The architecture of the Internet of Things system, and in particular the smart home, can be represented through three logical levels (fig. 1): the level of perception, the network level and the level of applications [1, 2]. Let's take a closer look at each level of the smart home system and analyze known cyber threats that violate the integrity, availability and confidentiality of information at the appropriate level.

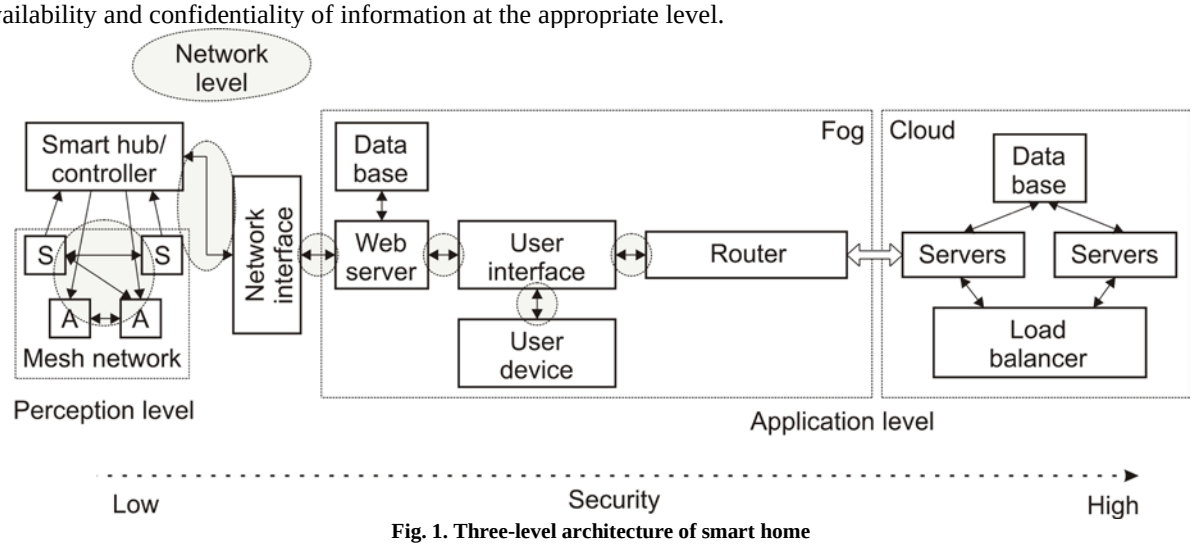

Fig. 1. Three-level architecture of smart home

Perception level

The closest level to the physical environment in the architecture of a smart home is the level of perception. The main functions of this level are the collection of information about the state of the physical environment and the implementation of mechanisms for influencing it. The assigned functions are implemented using multiple sensors and actuators, respectively. The information collected by the sensors depends on the nature of the physical environment and may relate to location, changes in the air and environment, movement, vibration, and so on. Actuators implement the principle of conversion of electrical energy transmitted through conductors into other types of energy. Examples of actuators are various types of motors, relay modules and automated cranes. The security of this level in the smart home system is the lowest, which «attracts» attackers to carry out attacks on the smart home device. The most common security threats to this level of perception are:

Eavesdropping. Eavesdropping is an unauthorized attack that violates the privacy of real-time information in which an attacker intercepts private messages, such as phone calls, text messages, fax transmissions, or video conferencing. Ehe main purpose of the eavesdropping attack is to violate the confidentiality of information. An unsecured data channel is used to access the information that is sent and received.

Fake node. This is an attack in which an attacker adds a new node to the system and fills the network with fake data. The main purpose of this attack is to stop the transmission of information from real network nodes. A node added by an attacker consumes the energy of real nodes and potentially controls it to destroy the network.

Node Capture. In this attack, an attacker gains full control of a key node, such as a gateway node. It can transmit all information, including the connection between the sender and the recipient, the key used to ensure secure communication and the information stored in memory.

Timing attacks: This is a type of passive attack aimed at devices with limited computing resources. During the attack, an attacker discovers vulnerabilities and obtains secrets that are stored in the security of the system, tracking how long it takes the system to respond to various requests.

Replay attack. This is an attack in which an attacker eavesdrops on security between the sender and the recipient and takes authentic information from the sender. The attacker sends the victim the same authenticated information that was already received during his communication, demonstrating proof of his identity and authenticity. The message is encrypted, so the recipient can consider it as a valid request and take the actions desired by the attacker.

Network level

The network layer performs a transport function for transmitting information within a smart home and is a bridge between the level of perception and the level of applications. It transmits information collected from physical objects using sensors. It also takes responsibility for connecting smart things, network devices and networks to each other. The presence of a communication component makes this level sensitive to attacks by attackers. It has noticeable [3, 4] security issues regarding the integrity and authentication of information transmitted over the network. Common security threats and problems for network layers are [5, 6]:

Expoloit: A type of attack that is implemented using a piece of software code or a sequence of commands that exploit vulnerabilities in software. The purpose of the attack can be both to seize control of the system and to disrupt its operation.

«Man in the middle» attack: A Man in the middle is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. One example of a MItM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Denial of Service (DoS) attack: This is an attack whose primary purpose is to prevent legitimate users from accessing devices or other network resources. This is usually accomplished by filling the target devices or network resources with redundant requests in order to prevent or complicate the use of some or all legitimate users.

Data Warehouse Attack: User information is stored on storage devices or in the cloud. An attacker could attack both storage devices and the cloud, and user information could be changed to incorrect information, thereby violating the integrity and confidentiality of data.

Application level

The application layer is the highest level in the logical smart home hierarchy and defines all applications that use smart home technology or in which smart home is deployed. Its main purpose is to provide services to applications. Services may be different for each program, as services depend on the information collected by the sensors. At the application level, there are many issues where security is a key issue. In particular, when the Internet of Things is used to create a smart home, it creates many threats and vulnerabilities inside and out. One of the main problems in implementing smart security in a smart home based on the Internet of Things is that the devices used in smart homes have low computing power and low memory. Common security threats and application level problems are [1, 7]:

Malicious code attack: This is code in any part of the software, the main purpose of which is to violate the confidentiality, availability and integrity of information, as well as damage to the system. Malicious software can implement its own code into the body of a user application, or exist separately in memory as a standalone software code, etc.

Cross-site scripting: This is an injection attack that allows an attacker to insert a client-side malicious code script, such as a web page viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. By performing such actions, an attacker can completely change the content of the program according to their needs and use the original information in an illegal way.

Smart home system security risk assessment

An important task in the design and operation of smart home systems is to identify cyber threats, assess their impact on potentially "bottlenecks" in the system and develop complete and comprehensive strategies to mitigate and eliminate the negative effects of cyberattacks. Moreover, the sooner the assessment is carried out and appropriate measures are taken, the greater the likelihood of ensuring the integrity, accessibility and confidentiality of information. Consider the process of assessing the risks of information security of the smart home system. To assess the risks, we use the OCTAVE Allegro methodology [9].

OCTAVE Allegro is a methodology that allows you to streamline and optimize the process of assessing information security risks, allowing the organization to obtain sufficient results in a small amount of time, human and other limited resources. The main focus of the OCTAVE Allegro methodology is to consider people, technology and tools in the context of their relationship to the information and business processes and services they support.

The OCTAVE Allegro methodology defines eight successive stages, organized in 4 phases (Fig. 2): definition of criteria, profiling of objects, identification of threats, identification and mitigation of risks. With the help of OCTAVE Allegro tables, it is possible to record the results of each assessment step risk and use them as input for the next steps. Individual steps apply to each individual information object. To assess safety risks, we use the OCTAVE Allegro template, which is presented in [9, 10].

During the research, we were inspired by work [10], and presented our own vision of the problem. Consider in more detail the application of the OCTAVE Allegro methodology to assess the security risks of a smart home system.

Definition of risk assessment criteria

The purpose of this step is to determine what may be the consequence of the risk to the business strategy and objectives or critical success factors (commercial stakeholders) and to the occupants of the smart home (non-commercial stakeholders). This step consists of two sub-step. The first sub-step involves defining a set of qualitative and quantitative measures to assess the impact of risks on the identified critical information objects in the smart home system. In the process of the second activity, the zone of influence is prioritized according to their importance for the owner of the smart home or stakeholders.

Criteria for evaluating the OCTAVE Allegro methodology include the following categories: customer reputation and trust; life, health, safety; fines and legal sanctions; financial losses; productivity.

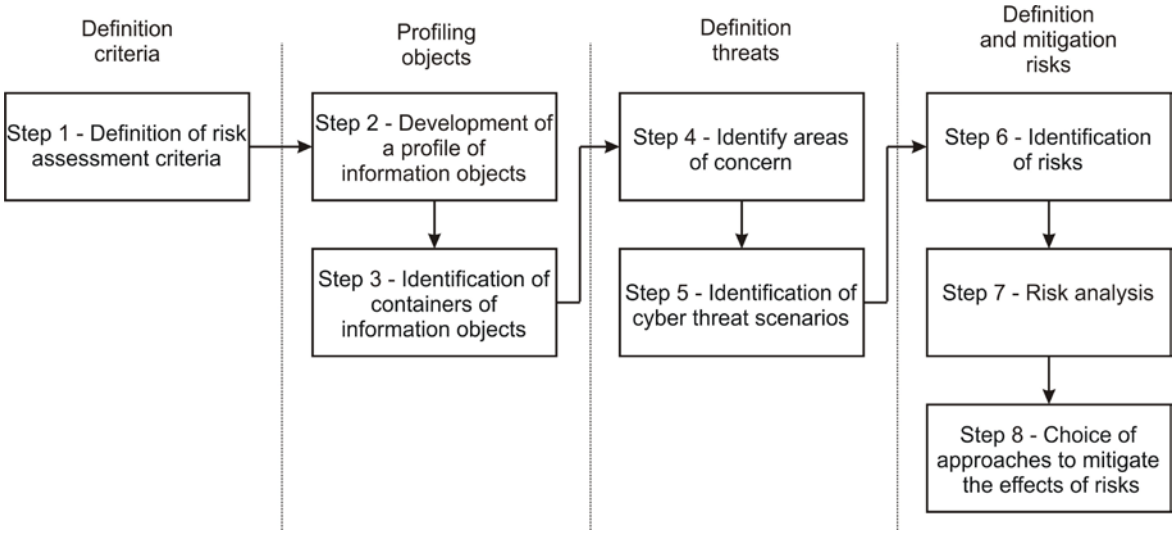

Fig. 2. Steps of the OCTAVE Allegro methodology

Before filling in the OCTAVE Allegro tables, it is necessary to determine who are the stakeholders for whom the risk assessment in the smart home system is carried out. The following stakeholders can be identified for the smart home system: non-commercial stakeholders represented by the end users of the smart home system and commercial stakeholders - software and hardware manufacturers, private and public companies involved in the installation and deployment of home automation systems, etc. Table 1 provides examples of risk assessment criteria, in particular for the categories of life, health, safety and fines and legal sanctions, as well as their priority.

Table 1

Risk assessment criteria

	Low	**Middle**	**High**
Criterion	Risk assessment criteria - life, health, safety (priority - 5)		
Life (non-commercial stakeholders)	No loss or significant threat to the lives of end users	Users' lives are in danger, but after receiving medical care, they recover	Loss of human life
Health (non-commercial stakeholders)	The deterioration is minimal and can be treated immediately with recovery within a few days	Temporary deterioration of users' health	Significant violation of the health of users. The recovery period is more than one month. Acquisition of chronic diseases.
Safety (non-commercial stakeholders)	The safety of the final consumer is in question	Minimal impact on end-user safety. The presence of an administrative offense	End-user safety is compromised. The presence of a criminal offense
…	…	…	…
Criterion	Risk assessment criterion - fines and legal sanctions (priority - 1)		
Fines (commercial stakeholders)	Collection of fines in the amount of less than UAH 100,000	Collection of fines in the amount of 100 to 300 thousand UAH.	Collection of fines in the amount of more than UAH 300,000.
Lawsuits (commercial stakeholders)	Registration of lawsuits in the amount of less than UAH 100,000	Registration of lawsuits in the amount of less than 100 to 300 thousand UAH	Registration of lawsuits in the amount of more than 300 thousand UAH.
Investigations (commercial stakeholders)	No inquiries from the government or other investigative agencies	Request for information from the government or other investigative body	The government or other investigative agency is launching an in-depth investigation against the stakeholders

Thus, the criterion for assessing the risks to life, health and safety is set at 5 (highest), for reputation - 4, for financial losses - 3, for productivity - 2. The lowest priority is the category of fines and legal sanctions with the appropriate level priority 1.

Development of a profile of information objects

In this step, critical information objects should be identified and profiled. In the process of profiling, we will define clear boundaries for the object in the smart home system, its safety requirements and identify all places where the object is stored, transported and stored. These steps will identify vulnerabilities in critical information objects.

The first step in the process of developing information object profiles is the actual identification of these objects. It should be noted that the level of applications will not be considered due to its greater security of information objects [8]. For the level of perception and network level of a smart home (Fig. 1), the following critical information objects can be distinguished [2]: information collected by sensors; video surveillance camera data; user credentials

(username and password); information resources (documents, user files); information on setting up a smart home; structure of a smart home (information about devices); information about the event log (information about the state of the smart home); user devices; location information. Table 2 shows the profile of the critical information object «information collected by devices»

Identification of containers of information objects

After describing the profiles of critical information objects, according to the OCTAVE Allegro methodology, the containers of information objects are identified. An information object container is a place where information is located. Containers can be technical (software, software, servers and communication networks), physical (paper, flash media, CDs) or people (who knows about the information). They can also be both internal and external to the organization. Let's analyze (technical, physical and human) containers for the critical information object «information collected by devices». Table 3 shows the containers of the information object «information collected by devices».

Table 2

Critical Information Object Profile "Information Collected by Devices (Sensors)"

(1) Critical object *What is a critical information object?*	**(2) Justification of the choice** *Why is this information important for the organization?*	**(3) Description** *What is the general description of this information object?*
Information collected by devices	This information object is an important component in the functioning of the smart home system and is the main source of input data on the state of the environment. Compromise of this information object may result in system malfunction and risks associated with, for example, fire or flood.	This information object determines the output from the devices, for example, it determines what actions the actuators will perform. This information determines the safety and convenience of the smart home, which are the main goals of the smart home system.
(4) Owner (s) *Who owns this information object?*		
The owner of this information object is the smart home system, which has the main responsibility for this information		
(5) Security requirements *What are the security requirements for this information object?*		
Confidentiality	Only authorized employees can view this information resource:	Only residents of the smart home have access to this information facility. This information may also be required by service providers for provision of appropriate services in accordance with contracts
Integrity	Only authorized users can modify this information object:	Only residents have the right to manipulate this information object.
Accessibility	This information object must be available to these users within 24 hours, 7 days a week.	This facility should be ready for use when residents or other related systems need it. This information facility must be available around the clock to ensure the operation of the smart home system. A short shutdown should not disrupt the operation of the system, while a long interruption (more than 8 hours) would cause significant problems.
(6) The most important safety requirements *What is the most important security requirement for this information object?*		
• Confidentiality	• Integrity	• Accessibility

Identify areas of concern

In this step the identify problem areas in previously identified information objects is carried out. For each identified information object, specific problems are identified that may adversely affect the security of this object. This step describes the potential impacts, if any, of the threat and the conditions that cause the event. The description, which is based on the storage locations of the information objects defined, provides a detailed understanding of where the information object may start a security breach.

Identification of cyber threat scenarios

The next step is to build threat scenarios for each identified information object. A threat scenario includes one or more objects, an actor (actor), means, motives, and a list of undesirable outcomes. An actor can be both natural (storm, flood, fire or other disaster), automated (malicious software) and intelligent (criminal, activist or other person who intends to cause school to a smart home). The means is the vulnerability used by the entity against the information object. The motive is the actor's desire to apply the means to the information object. An undesirable result is damage to the information object (it can be disclosure, alteration, interruption or destruction). This step allows to identify threat scenarios that can be implemented to a greater extent. Threats are identified using containers in which object are stored or transferred.

Table 3

Containers of the information object "information collected by devices (sensors)"

№	Description of the container	Owner
Technical information containers		
Internal		
1 2 3	Database: The information resource is located on database servers and web servers The internal network of a smart home User's devices	Smart home owner / residents
External		
5	Internet	–
Physical information containers		
Internal		
1 2	Paper media Storage devices	Smart home owner / residents
External		
–	–	–
Human information containers		
Internal		
1	Family members	residents
External		
2 3	Guests Service man	Guests Service man

Identification of risks

Risk is the possibility of causing damage or loss (data, software, hardware) and consists of event, consequence and uncertainty. The threat can have many potential negative consequences for the organization. For example, a breach of an organization's e-commerce system can affect an organization's reputation with customers as well as its financial position. In order to determine the risks for each information object, a threat scenario is applied to its components, provided that the threat scenario is implemented and the impact on the stakeholders of the smart home is assessed.

Risk analysis

At this stage, the identified risks in step 6 are assessed using the assessment criteria established in the first step. These scores are used to prioritize risks, and as a result, to mitigate the impact of risks on the smart home system. Thus, for each risk of the information object, the following actions should be performed: assign values "high", "medium" and "low" in the field Value (Table 4) taking into account the risk assessment criteria (Table 1); calculate the score for each impact zone by multiplying the impact area priority by the impact value (high = 3, medium = 2, low = 1). After writing the result in the evaluation column, a final evaluation is formed, which is a relative indicator of risk.

Choice of approaches to mitigate the effects of risks

In the latter, the risks analyzed in the previous step are used to develop a strategy to mitigate the potential impact of risks on the information objects of the smart home system. Thus, in this step, the approach is chosen to deal with each threat according to their priority. There are several approaches to the choice: accept, reduce, transfer, postpone. After identifying the risks and assessing the risks, a mitigation checklist can be defined to avoid or limit the identified risks and the negative consequences arising from them. We perform a risk assessment for the information object «information collected by devices» (Table 4).

These steps of the OCTAVE Allegro methodology are performed for each critical information object. The conducted risk assessment process allows to analyze information objects in the smart home system that are critical from the point of view of safety, to analyze risks and their effects on objects, and to suggest possible countermeasures to protect information objects and create a smart home system more safer.

Conclusions

As a result of the study, the architecture of a smart home was considered as a system consisting of three logical levels: perception, network and application level. A review of known cyber threats was conducted for each level. In particular, critical information objects in the smart home system, risk assessment criteria and cyber threat scenarios have been identified. The information security risks of the smart home system were assessed using the OCTAVE Allegro methodology for the information object that presents the information collected by the smart home sensors. Further research is the formation of a comprehensive risk assessment of information security of the smart home system and the implementation of the software system, which will automate the process of risk assessment not only for the smart home system, but also for other systems that implement the Internet of Things.

Table 4

Risk assessment for the information object «information collected by devices»

Risk Threat	**Information object**	Information collected by devices

		Area of concern	1) Changing the gas sensor can lead to a wrong response to the presence of gas in the room, which can affect the health and lives of residents 2) Obtaining data from the motion sensor can be used to determine the presence of occupants of the house. 3) Reading the status of door locks and alarm systems can be used to determine when a smart home is busy. 4) DoS attacks on the smart home system do not produce the ability to perceive the physical parameters of the sensors, which makes it impossible to detect such risks as fire, floods, unexpected movements, and so on			
		(1) Actor *Who will influence the information object creating a security threat?*	Intruder (hacker, unscrupulous supplier of software and hardware)			
		(2) Means *How will the protagonist do this? What should they do for this?*	Hacking tools Vulnerabilities in hardware			
		(3) Motive *What benefit does the protagonist gain from a security breach?*	Financial benefit, satisfaction of personal ambitions.			
		(4) The result *How will this be reflected in the information object?*	o **Disclosure** • **Modification**		o **Destruction** • **Interruption**	
		(5) Safety requirements *How will the security requirements of the information object be violated?*	This information should only be available to smart home owners			
		(6) Probability *What is the probability of reproducing such an effect?*	• **High**	o **Medium**	o **Low**	
	(7) Consequences *What will be the consequences for the organization or owner of the information object in case of violation of security requirements?*		**(8) Difficulty** *How serious are these consequences for the organization or owner of the facility, depending on the area of influence?*			
	In case of violation of safety requirements for this information object, the smart home system will not be able to monitor and control critical indicators of sensors, which can lead to negative consequences related to both the physical nature (fire, flooding) and the human factor. (penetration, theft of things). In both cases, the manifestations of negative consequences can lead to large financial losses		**Impact area**	**Value**	**Score**	
			Customer reputation and trust (4)	Middle (2)	4*2 = 8	
			Financial losses (3)	High (3)	9	
			Productivity (2)	Low (1)	2	
			Life, health, safety (5)	High (3)	15	
			Fines and legal sanctions (1)	Low (1)	1	
Relative value of risk assessment						35
(9) Risk mitigation Based on an overall assessment of this risk, what actions should be taken?						
o **Accept**	o **Defer**	• **Mitigate**	o **Transfer**			
The following steps should be taken to mitigate the risks that have been identified						
Which container will the action apply to?	*What administrative, technical and physical controls should be applied to this container? What residual risk will the organization still accept?*					
Technical	Restrict the availability of network traffic only to authorized users; use of encrypted data transfer protocols (e.g. SSL / TLS)					
Physical	Store all physical data in a safe place. Regular hardware updates; back up all important information.					
People	Informing residents about the safe management of a smart home					

References

1. Burhan M. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey / M. Burhan, R.A. Rehman, B. Khan, B.S.Kim // Sensors (Basel) – 2018. – 18(9):2796.

2. Sethi P. Internet of Things: Architectures, Protocols, and Applications / P. Sethi, S.R. Sarangi // Journal of Electrical and Computer Engineering. – 2017. – 25 p.

3. Al-Garadi M. A. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security / M.A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, M. Guizani // arXiv:1807.11023. – 2018.

4. Apthorpe N. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic / N. Apthorpe, D. Reisman, N. Feamster // arXiv:1705.06805. – 2017.

5. Nicheporyk A.O. A method of detecting DDoS attacks on an IoT network / O.A. Nicheporyk, A.A. Nicheporyk, O.V. Fegir, A.D. Kazantsev, Ю.О. Nicheporyk // Bulletin of Khmelnytsky National University. Series: Technical Sciences. Khmelnytskyi. – 2020. – № 1. – P.156-164 [in Ukrainian].

6. Lee I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet. 2020; 12(9):157. https://doi.org/10.3390/fi12090157

7. Zhao S. Computational Intelligence Enabled Cybersecurity for the Internet of Things / S. Zhao, S. Li, L. Qi and L. D. Xu, // Proceedings of IEEE Transactions on Emerging Topics in Computational Intelligence. – vol. 4. – № 5. – P. 666-674.

8. Sarrab M. / Critical Aspects Pertaining Security of IoT Application Level Software Systems / M. Sarrab and S. M. Alnaeli, // Proceedings of 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). – 2018. – P. 960-964.

9. Caralli R.A. Octave allegro: Improving the information security risk assessment process / R.A. Caralli, J.F. Stevens, L.R. Young, W.R. Wilson // Technical report. – Software Engineering Institute, CMU/SEI-2007-TR-012, 2007.

10. Ali B. Internet of Things based Smart Homes: Security Risk Assessment and Recommendations / B. Ali // Master's Thesis, Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering, 2016, 98 p.