УДК: 004.056.53
https://doi.org/10.47533/2023.1606-146X.40

***S. T. TLEUBERDIN*, Y. N. SEITKULOV***

*L.N.Gumilyov Eurasian National university,*
*Astana, Kazakhstan*
*sakentleuberdin@gmail.com, yerzhan.seitkulov@gmail.com*

# CLASSIFICATION OF CYBER THREATS FOR INTERNET OF THINGS

*Smart home consists of various Internet of things (IoT) devices. These IoT devices are designed to help and simplify people's lives. The technical progress of the IoT field is aimed at simplifying human life, thereby creating new cyber threats. Different scientific papers are mentioned that number of IoT devices is growing constantly by 15% per year. As a result, around 1.6 billion IoT devices will be used globally over the internet. It means that IoT devices will be accessed over internet by consumers. Nowadays, Internet is accessible easily by everyone, so they can afford freely the ecosystem of IoT devices at home. Within this development of IoT ecosystem, consumers can face serious problems of transmission and storage of information by IoT devices. These problems might be data theft from IoT devices, using such IoT devices for Denial of Service (DoS) attacks, user tracking and so on. Local cyber threats provide an opportunity for an attacker to gain access to a home network and take advantages of it. Global cyber threats are dangerous because IoT devices can be controlled remotely from anywhere in the world without the knowledge of the user. One of the risks is that the user's home network of IoT devices could be controlled by botnets to carry out cyber-attacks. The article describes and analyzes current threats to IoT smart home devices and provides examples of data collected and processed by smart devices. Collecting information about users through IoT devices is a novelty of this work.*

***Keywords****: IoT devices, smart home, IoT cyber threats, security of IoT devices, data security, classification of cyberthreats; security of smart devices.*

**Introduction.** The Internet of Things (IoT) is a unified network of devices that interact with each other and with the outside world to transmit and process data. IoT devices can have installed software and built-in sensors for transmitting information to the global network or for interacting with devices in a local network [1]. The Internet of Things system helps to simplify everyday life tasks, thereby providing dynamism and convenience for people's lives. For example, IoT devices as part of a smart home help turn off the lights in the absence of a person in the room, the temperature in the house may vary depending on the parameters set by the owner of the house. Additionally, home Internet of Things devices can interact with each other and provide various services to users. For example, a smart assistant can play a song from the owner's audio library or help launch certain actions on other IoT devices based on everyday tasks stored in the smart assistant's memory.

**Research methodology.** Infocommunication between IoT devices can be defined as an ecosystem that consists of several important components. These IoT devices interact with each other and create an ecosystem to provide certain services to users.

Description of parts of the IoT ecosystem:

• An IoT thing is a physical object that can be detected and combined into a local network. IoT things necessarily function to transfer information over a local network among themselves. Additionally, they can transfer data to cloud services to process this data. More

* E-mail корреспондирующего автора: sakentleuberdin@gmail.com

multifunctional things perform additional tasks, such as collecting information, computing based on installed software, interacting with cloud services to perform various functions, visualizing the map and storing it in memory to solve problems, etc. [2].

• Decision–making is a decision-making process based on data that is transmitted from IoT devices. Multifunctional IoT devices are capable of storing big data, can also process and analyze it. The most necessary thing for this process is the availability of the necessary information, since decisions will be made on the basis of the information provided [3]. This process is very important for the IoT ecosystem, because the results of the decisions made contribute to the creation of new actions for IoT devices. It is important to note that information analysis for decision-making can function locally or through interaction with cloud applications.

• A sensor is an important object of the IoT ecosystem that helps to function in the environment. Sensors are easily installed in physical objects as they are very flexible and small in size [4]. Sensors can be divided into levels such as physical and digital. At the physical level, sensors can detect various indicators and diagnose changes in the environment. At the digital level, sensors collect all the necessary data in a local network. Thus, sensors create data obtained from the environment for subsequent tasks of the IoT ecosystem. Such as sensors for measuring temperature and pressure, accelerometers and acoustic sensors. Sensors are extremely necessary in the IoT ecosystem of a smart home for collecting and processing information [5].

• Actuators are objects that perform the function of signal conversion to control the mechanism. Thus, the mechanism operates in the reverse direction from the sensor [6]. As an example, we can take the mechanism of operation of smart lamps, where the signal coming from the sensor is used to adjust the brightness level of the lamp.

• One part of the IoT ecosystem is embedded systems. This means that IoT devices are designed with installed sensors and operating mechanisms that provide the ability to connect to a local network, run software and may have a memory capacity for data storage. Also, such IoT systems are created on certain processors, which will provide the opportunity to function and store data independently. For example, smart watches, vacuum cleaners, virtual assistants, refrigerators, etc. They belong to embedded systems because they can work both independently and interact with other IoT devices [3].

• Communication is an integral part of the IoT ecosystem for data transmission and for interaction in a local network. The types of communication in IoT devices vary greatly depending on the functions and resource requirements [7]. Thus, the choice of a communication protocol for the IoT ecosystem depends on the goals and objectives of use. In practice, IoT ecosystems use different communication protocols using a common router to provide IoT device compatibility. Communication between IoT devices relies on the ability to transmit and receive data in an orderly manner. In IoT ecosystems, communication can be wireless and wired. In practice, wireless communication is often used in IoT ecosystems due to the flexibility and cost-effectiveness of this technology. Wireless communication has different properties such as signal range, bandwidth, security, quality of service, etc. Also, wireless technologies can be classified as short-range contactless communication, personal network, local area network, regional network and global network [8].

**Practical results.** The concept of a smart home includes a stack of technologies that help to save human time and resources lost on household chores. The complex of technologies used facilitates the interaction of home IoT devices and helps to perform various actions without human intervention. For example, automatic switching on and off of lights in a room in the absence of a person, automatic regulation of room temperature, smart notification when theft attempt is detected, automatic water shutdown in case of leakage and so on. Considering the constant development of smart home concepts, new software solutions and IoT devices for home use are being actively developed [8].

With the active growth of IoT devices in the smart home concept, it is necessary to pay special attention to cyber threats to the IoT ecosystem. Smart devices can transmit, process and store confidential information about their owners. Smart IoT devices may be vulnerable to various attack vectors. Thus, the confidential information of the owner of these devices may end up in the hands of cybercriminals [9].

It is necessary to visualize the topology of the local network used to analyze IoT cyber threats. In practice, wireless communication is very often used to transmit data in a local network [10]. Such wireless technologies are most often Wi-Fi, Bluetooth and infrared channel (IR). Also, devices are often used to control signals within the network, such as a smartphone, router and cloud server. In a typical topology, a smartphone is used to manage IoT devices and to change device settings, a router to automate the process of managing devices on a local network, and a cloud server in cases of remote control of device settings. It is necessary to consider the levels for studying IoT threats. Cyber threats can be at the level of a cloud service, the operating system of a smartphone and router, and at the level of wireless communication.

Table 1 shows the components of the smart home It ecosystem with a description of the data that IoT devices transmit on the local network. Also, information is provided about the communication methods of these smart devices and describes how to identify the user and get information about the user.

***Table 1*** – Smart home components

| IoT devices | Transmitted data | Communication method for data transmission | User recognition and user information acquisition |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Smart light bulbs and table lamps | - Manufacturer<br>- device model<br>- device ID<br>- firmware version<br>- Name of the item<br>- location by house<br>- power consumption<br>- current voltage in the network<br>- the script for starting the device<br>- device operation schedule | Commands for device management can be executed locally or remotely. Accordingly, Wi–Fi connection is supported in many manufacturers. Data from these devices is transmitted throughout the local network. | With the help of data, it is possible to determine the presence or absence of tenants in the apartment, the time zone at which the device operates [11]. |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Smart Floor Scales | - Manufacturer<br>- device model<br>- device ID<br>- user profile<br>- health and weight tracking with data recording function | Smart scales work on wireless technologies like Wi-Fi and Bluetooth. User data is transmitted to the controlling smartphone. | Information about the user's health status [11]. |
| Smart Sockets | - Manufacturer<br>- device model<br>- device ID<br>- firmware version<br>- Name of the item<br>- location by house<br>- power consumption- - current voltage in the network<br>- the script for starting the device<br>- status of the current state | Smart sockets accept commands over a Wi-Fi network from a router (a single managed gateway) or a smartphone.<br>Data from these devices is transmitted throughout the local network. | When finding the power consumption status, it is possible to determine the type of charger that is connected to the network, as well as when analyzing groups of outlets to determine the number of connected devices in the apartment [11]. |
| Climate control items | - Manufacturer<br>- device model<br>- device ID<br>- location by house<br>- power consumption<br>- the script for starting the device<br>- status of the current state<br>- room temperature<br>- humidity level | Such items receive commands over a Wi-Fi network from a router (a single managed gateway) or a controlling smartphone. Data from these devices is transmitted throughout the local network. | Information is transmitted about the locations of devices, the level of pollution inside and outside the room. It is possible to determine the user's climatic preferences and detect the area of residence [12]. |
| Teapot | - Manufacturer<br>- device model<br>- device ID<br>- power consumption<br>- status of the current state<br>- water temperature | The smart kettle receives commands over the Wi-Fi network from the gateway or the controlling smartphone. The initial settings are synchronized in the smartphone. | When processing information, you can find out the frequency of the kettle and thereby determine the presence of a person in the apartment [13]. |
| Iron | - Manufacturer<br>- device model<br>- device ID<br>- power consumption<br>- location<br>- temperature indicator<br>- status of the current state | A smart iron can transmit information over a Wi-Fi network and receive commands from a gateway or a controlling smartphone. | When processing information, you can find out the location of the device and remotely control the modes of the iron for the purpose of arson [13]. |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Vacuum cleaner | - Manufacturer<br>- device model<br>- device ID<br>- power consumption<br>- location<br>- status of the current state<br>- a map showing the items located in the apartment<br>- working OS and software used<br>- recording of the apartment plan | The vacuum cleaner can be controlled remotely via a smartphone or via a control gateway. The Wi-Fi network is used to receive commands from the user and to update the software from the manufacturer. | A smart vacuum cleaner uses lidars to avoid colliding with objects inside the house and store this data in memory. Accordingly, a person's conversation may be stored in the vacuum cleaner's memory due to the vibration of the voice[14]. Also, the vacuum cleaner uses built-in sensors indicating the distance from objects to draw up a plan of the room and the objects located. Thus, with remote control of the vacuum cleaner, you can find out the presence or absence of people in the apartment [13]. |
| Washing machine | - Manufacturer<br>- device model<br>- device ID<br>- power consumption<br>- status of the current state<br>- audio recording of the owner's voice<br>- used software | The washing machine can be controlled remotely via a smartphone or via a control gateway. The Wi-Fi network is used to receive commands from the owner. | Modern smart washing machines have the function of recording the owner's voice to control the washing modes. Thus, it is possible to identify the owner's voice when hacking the device [12]. |
| Smart TV | - Manufacturer<br>- device model<br>- device ID<br>- power consumption<br>- location and IP address<br>- status of the current state<br>- working OS and software used<br>- User data, subscriptions and payment information<br>- Access to social accounts<br>- User speech recognition for management | A smart TV can be controlled remotely via a smartphone or via a control gateway. The Wi-Fi network is used to receive commands from the user and to update the software from the manufacturer. | When hacking a smart TV, you can get stored audio information, as well as perform remote surveillance. Also, you can get a personalized user content [12]. |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Fridge | - Manufacturer<br>- device model<br>- device ID<br>- power consumption<br>- status of the current state<br>- Used software<br>- information about stored products in the refrigerator | A smart refrigerator can be controlled remotely via a smartphone or via a control gateway. The Wi-Fi network is used to receive commands from the user and to update the software from the manufacturer. | When processing information, it is possible to obtain information about stored human products, thereby finding out the material status of the user and with a detailed analysis, it is possible to determine the state of human health. Also, with certain refrigerator functions enabled, you can find out the absence of the owner[13]. |
| Voice Assistant | - Manufacturer<br>- device model<br>- device ID<br>- power consumption<br>- location and IP address<br>- status of the current state<br>- working OS and software used<br>- User data, subscriptions and payment information<br>- Access to social accounts<br>- User speech recognition for management<br>- centralized management of It devices | The voice assistant can be controlled remotely via the user's smartphone. The Wi-Fi network is used to receive commands from the user and to update the software from the manufacturer.<br>The voice assistant controls other IoT devices via Wi-Fi and Bluetooth and acts as a gateway for device management. | When you get access to the voice assistant, you can fully control IoT devices of the smart home. Accordingly, we get the location of all devices in the local network, a map of the premises, access to personal data and subscriptions, an archive of user requests and commands[12]. Also, you can perform surveillance on the user and record audio conversations. |

**Classification of IoT device threats.** To describe the threats associated with the IoT ecosystem of a smart home, it is necessary to understand the main assets that need protection[8]. The assets that need to be protected are listed in table 2.

***Table 2*** – Assets requiring protection from cyber threats

| Group | Assets | Description |
|---|---|---|
| 1 | 2 | 3 |
| IoT devices | Sensors | Sensors are used to detect and measure parameters in the environment. The actuators perform the function of transferring data to other IoT devices |

| 1 | 2 | 3 |
|---|---|---|
| | Software and operating system | Ensures the operation of the application on an IoT device. |
| | Embedded systems | Multifunctional devices that can process data and run applications locally, write data to memory. |
| Infrastructure | Gateway | A component of the IoT ecosystem for managing and interacting with all connected devices on a local network. |
| | Power supply | Provides electricity for IoT devices on the network. |
| | Smartphone | The user's device for managing and configuring all IoT smart home devices |
| Link | Network | There are different types of networks with different characteristics. The most used type of network for a smart home is a local area network (LAN). |
| | Protocols | They are used to create a common language of communication between devices. Depending on IoT devices, there are different types of communication protocols that can be wired and wireless. |
| Information | Data | User data can be stored locally on devices or in a cloud server. Also, there is data that is transmitted in the local network between IoT devices. |

After determining the assets that need to be protected, it is necessary to identify cyber threats to the IoT devices of the smart home. Thus, cyber threats can be divided by the type of impact and by the type of network topology on IoT devices. According to the type of topology, it can be divided into types such as local, global and vulnerable software [3]. Local cyber threats are described as the actions of a hacker who needs to be near a smart home to intercept data that is transmitted wirelessly. Thus, an attacker can hack the user's Wi-Fi network or the Bluetooth protocol to gain access to IoT devices. Global cyber threats target cloud servers of the manufacturer of IoT devices that store and process user data. Manufacturers of smart IoT devices are the main target of attackers because it makes it possible to obtain customer data from around the world and hackers can also influence IoT devices globally. For example, they will be able to disable the update database for smart devices or

introduce malicious code through the update function. The latter type of cyber threats is associated with vulnerabilities in the software and OS of smart devices, smartphones, routers, etc. Vulnerabilities allow an attacker to gain remote or local access to IoT devices, read data records and control these smart devices.

**Practical experiment.** I would like to discuss an experiment that have been deployed to show practical IoT attacks to IoT devices. I decided to use a software to simulate IoT home devices. Simulated IoT devices connected to internet in order to collect various type of attacks.

Technically, the host is connected to Internet and it has a public IP address. I open 21 and 22 ports for Telnet and SSH services. In this case, it is allowed to login with a default password such as "root:root" for both services. I created a device and named it as "home-bedroom". This is simulated IoT device that is a part of the simulated home network. Once attacker will obtain session on the system, it gets root privileges in order to download malicious software and to expand network scanning. I propose that attackers gain accesses to the simulated IoT device, finding vulnerabilities by scanning the home network and executing malicious files. It is a common thread for IoT home devices.

I present the typical model of IoT home environment that is connected to Internet in figure 1. It is very simple and common way to have IoT home network. Commonly, all IoT devices are connected to the internet in order to communicate with an owner.

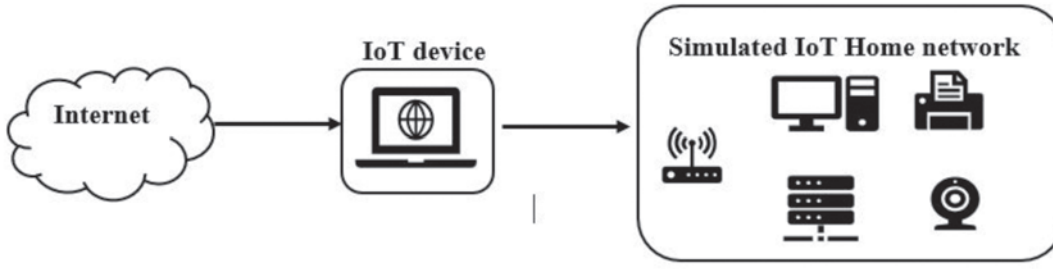


***Figure 1*** – typical model of IoT home network

I described tools and programs that simulates IoT environment in table 3.

***Table 3*** – Components of simulated IoT environment

| Components | Description |
|---|---|
| BevyWise software | Simulation of IoT devices |
| Cowrie | Virtual environment for python |
| Oracle VM Virtual Box | It is used to deploy virtual machines and configure connections between them. |
| Lenovo Thinkpad laptop | It is used to run and manage operations |

I collected attack data from various hosts that are connected to my simulated IoT device. I figure out that there are main four phases that can be observed from the attacked data. It is obviously that attackers scan public IP addresses every 15 minutes for open ports, executing

brute force attacks to find valid accounts and then gaining access to the system. The main observable phases for this experiment are described in table 4.

***Table 4*** – Four main observable attack phases

| Attack phase | Description |
|---|---|
| Reconnaissance | Scanning massively public IP addresses to find out open ports |
| Intrusion | Executing brute force attack based on dictionary to find valid accounts |
| Persistence | Using a valid account to have access for IoT device. Installing executable files to deploy various services on the system |
| Command and Control | Using tools to control IoT device remotely. Using this system and its resources to attack other systems. |

**Conclusion:** There are cyber threats associated with smart home IoT devices that can affect human security based on the above information. Thus, smart home IoT devices can carry cyber threats as they collect and process sensitive user data. When collecting and analyzing data transmitted between IoT devices, it is possible to create a profile of a smart home user, thereby creating a cyber threat to the user. Also, it should be noted that the more IoT devices in the network, the greater the risk of identifying a smart home user and the greater the chances of successful hacking of the home network. To minimize the risks of hacking and leakage of sensitive data, components, smart home assets and types of cyber threats for IoT devices were provided. Additionally, examples of scenario attacks on IoT devices with a degree of risk of attacks are presented. All this information shows the current threats of smart home IoT devices that exist and require special attention for further study. I provided the experiment results that showed that IoT device that is connected to Internet will be scanned within 15 minutes by attackers. I described four main phases that I figure out during this experiment that is related to IoT home security. From this experiment, I obtained information that is related to attacker's geolocation, behavior and tools that are used to attack the simulated IoT device.

## REFERENCES

1 Aldhaheri, S., Alghazzawi, D., Cheng, L., Barnawi, A., & Alzahrani, B. A. (2020). Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research. Journal of Network and Computer Applications, 157, 102537

2 Abu Al-Haija, Q., & Zein-Sabatto, S. (2020). An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. Electronics, 9(12), 2152.

3 Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., & Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. Simulation Modelling Practice and Theory, 101, 102031.

4 Babun, L., Denney, K., Celik, Z. B., McDaniel, P., & Uluagac, A. S. (2021). A survey on IoT platforms: Communication, security, and privacy perspectives. Computer Networks, 192, 108040.

5 Chmiel, M., Korona, M., Kozioł, F., Szczypiorski, K., & Rawski, M. (2021). Discussion on iot security recommendations against the state-of-the-art solutions. Electronics, 10(15), 1814.

6 Ghimire, B., & Rawat, D. B. (2022). Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. IEEE Internet of Things Journal.

7 Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. Internet of Things, 15, 100420.

8 Koohang, A., Sargent, C. S., Nord, J. H., & Paliszkiewicz, J. (2022). Internet of Things (IoT): From awareness to continued use. International Journal of Information Management, 62, 102442.

9 Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., ... & Cui, L. (2020). Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. Measurement, 154, 107450.

10 Mahbub, M. (2020). Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. Journal of Network and Computer Applications, 168, 102761.

11 Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. (2020). A comprehensive and systematic survey on the internet of things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers, 9(2), 44.

12 Sarica, A. K., & Angin, P. (2020). Explainable security in SDN-based IoT networks. Sensors, 20(24), 7326.

13 Sami, S., Dai, Y., Tan, S. R. X., Roy, N., & Han, J. (2020, November). Spying with your robot vacuum cleaner: eavesdropping via lidar sensors. In Proceedings of the 18th Conference on Embedded Networked Sensor Systems (pp. 354-367).

14 Larriva-Novo, X., Villagrá, V. A., Vega-Barbas, M., Rivera, D., & Sanz Rodrigo, M. (2021). An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets. Sensors, 21(2), 656.

15 Viejo, A., & Sánchez, D. (2020). Secure monitoring in IoT-based services via fog orchestration. Future Generation Computer Systems, 107, 443-457.

***С. Т. ТЛЕУБЕРДИН, Е. Н. СЕЙТКУЛОВ***

*Л.Н. Гумилев атындағы Евразиялық ұлттық университеті,*
*Астана қ., Қазақстан*

## ЗАТТАР ИНТЕРНЕТІНЕ АРНАЛҒАН КИБЕРҚАУІПТЕРДІҢ КЛАССИФИКАЦИЯСЫ

*Ақылды үйдегі IoT құрылғылары адамдардың өмірін жеңілдетуге және көмектесуге арналған. IoT саласындағы техникалық прогресс адам өмірін жеңілдетуге байланысты жаңа киберқауіптерді тудырып отыр. Жергілікті киберқауіптерлер шабуылдаушыға жергілікті үй желісіне қол жеткізуді және өзіне пайда алу мүмкіндігін туғызады. Жаһандық киберқауіптер өте қауіпті, себебі пайдаланушының IoT құрылғыларын хабарынсыз әлемнің кез келген нүктесінен қашықтан басқаруға болады. Тәуекелдің бірі, бұл пайдаланушының IoT құрылғыларынан тұратын үй желісі ботнеттермен басқарылып және басқа кибершабуылдарға қолдануы мүмкін. Осы мақалада ақылды үйдегі IoT құрылғыларына қатысты өзекті қауіптер сипатталған және смарт құрылғылар жинайтын және өңдейтін деректер мысалдары берілген. IoT құрылғылары арқылы пайдаланушылар туралы ақпарат жинау – бұл жұмыстың жаңалығы.*

***Түйін сөздер****: IoT құрылғылары, ақылды үй, IoT киберқауіптері, IoT құрылғыларының қауіпсіздігі, деректер қауіпсіздігі, киберқауіптердің классификациясы.*

***С. Т. ТЛЕУБЕРДИН, Е. Н. СЕЙТКУЛОВ***

*Евразийский национальный университет имени Л.Н.Гумилева,*
*г. Астана, Казахстан*

## КЛАССИФИКАЦИЯ КИБЕРУГРОЗ ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

*IoT устройства умного дома созданы помогать и упрощать жизнь людям. Технический прогресс IoT области нацелен на упрощение жизни человека, тем самым создавая новые киберугрозы. Локальные киберугрозы предоставляют возможность злоумышленнику получить доступ в домашнюю сеть и извлекать для себя выгоду. Глобальные киберугрозы опасны тем, что IoT устройства могут управляться удаленно из любой точки мира без ведома пользователя. Одним из рисков является то, что домашняя сеть пользователя, состоящая из IoT устройств, может быть захвачена ботнетами для проведения кибератак. В данной статье описаны и проанализированы актуальные угрозы для IoT устройства умного дома и приведены примеры о данных, которые собирают и обрабатывают умные устройства. Сбор информации о пользователях через IoT устройства является новизной данной работы.*

***Ключевые слова****: IoT устройства, умный дом, киберугрозы IoT; безопасность IoT устройств; безопасность данных; классификация киберугроз.*