UDC 004.7:007.5:004.4

RESEARCH AND DESIGN OF AN AUTOMATED MULTIFUNCTIONAL SYSTEM FOR THE SMART HOUSE TECHNOLOGY

S. I. Hapii[1], R. L. Tkachuck[2]

[1]Lviv Polytechnic National University,
12, Bandera St., Lviv, 79013, Ukraine

[2]Lviv State University of Life Safety,
35, Kleparivska St., Lviv, 79007, Ukraine

One of the main functions of the Smart House system is to ensure the security and integrity of different types of objects (buildings, surrounding areas, individual rooms, and different types of transport, etc.). It is established that the main conditions for the effectiveness of security systems are the choice of the best set of sensors and their installation. In addition, the basis of the success of these systems is a highly functional system for alerting and responding to various problems. The main problems of security systems are considered, their research is carried out and the optimal ways of solving the protection of objects are offered. The expediency of the development in the field of defence is considered, the prospects of this development are evaluated and substantiated, and its improvements in the future are described. The developed program is presented, its functionality is described, and the expediency of this development is justified.

Keywords: *cyber defence, security system, sensors, alerts, security.*

Introduction. Throughout the entire history of mankind, in addition to changing activities, work routines, a set of random ideas, discoveries, and revolutionary changes in life, it sought one constant thing – a sense of safety and security. In addition, with the course of history, the ways of meeting this need have changed and evolved along with humanity. Instead of fortresses and armoured guards, there are uniformed guards at the entrance document checks, metal detectors instead of a person to search, and means of instant alarm instead of a loud bell in the nearest tower. Security needs are changing, and the requirements for it are only growing.

In independence, in which field of activity a person is involved, peace, security, and privacy of his life. The manifestation of these things can be seen in people's caution, whether it is a more complex account password, multiple door locks instead of one, or the habit of keeping valuables in the least accessible pockets. One can feel calm only at home, and then on the condition that your home is your fortress. And to make it a fortress will still have to make efforts. Of course, reinforced doors, multiple locks, and the presence of an owner in the house can ensure the security of the property, but what about the situation when no one is at home? Picking locks is a common practice for thieves, but it will delay them for some time. Fortified doors, on the contrary, can play

the role of bait, even in a situation where it was not possible to bypass the locks, no one cancelled the brute force method. An intruder will come across an alarm system, and in the best case he will leave the house in fear of being caught, the second option is to grab only expensive things and run away, there are even certain statistics that a professional thief needs about 7 minutes to get all the most valuable things. And this is considered a rather successful situation.

Formulation of the problem. Throughout his life, every person on Earth earns property, but there were always those who wanted to steal or damage this property. Therefore, throughout history, people sought to ensure the safety of these values. Over time, all systems improved, iron bars were replaced by laser motion detectors, guards at the door with alarms, and video surveillance cameras. Today, there are many systems for providing protection, from the cheapest with moderate functionality to the most expensive, the work of which ensures the complete security of the client's property.

According to the law of Ukraine [8]:

- the object of protection – a natural person and/or property;
- the subject of security activity - a business entity of any form of ownership, created and registered on the territory of Ukraine, which carries out security activities based on a license obtained in accordance with the established procedure;
- property protection – activities related to the organization and practical implementation of protection measures aimed at ensuring the inviolability and integrity of the buildings, structures, territories, water areas, vehicles, currency values, securities, and other movable and immovable property specified by the owner and belonging to him, with the aim of preventing and/or preventing or stopping illegal actions against it, to preserve its physical condition, stop unauthorized access to it by the owner and ensure that the owner of this property exercises all the powers that belong to him in relation to it.

Today, there is a need for a security system that will have high efficiency and will be able to provide high security to the object under surveillance.

Analysis of the relevance of the work.

Analysis of existing solutions in smart home communication protocols. The number of electrical appliances in a household is steadily increasing. Their total power can reach 15 kW. At the same time, the network capacity is limited and usually does not exceed 10 kW. That is, when most of the appliances are connected simultaneously, the household is disconnected from the grid in an emergency. Moreover, electricity consumption in households is unevenly distributed throughout the day [3]. This problem leads to an imbalance in the state power system, the need to manoeuvre the generated capacities (construction of new PSPPs, regulation of the capacity of existing TPPs and HPPs), as well as to outages of large consumers in peak modes, resulting in a decrease in the efficiency and reliability of the entire power system, and billions of dollars in costs for the state, private producers and consumers. To encourage partial balancing of energy consumption in households, the government introduces multi-zone electricity tariffs (two- and three-zone). However, it is impossible to use this incentive to the fullest extent in a household without a simple and reliable Smart Home system that would allow automated control of electrical appliances depending on the current state of the home

energy system. Today, there are a huge number of tools for controlling and monitoring the operation of household devices, such as smart sockets, smart meters, and others. However, they do not have a systematic approach to solving the problems described above: the decision to turn on/off a particular appliance is often made manually by the user, and there are no opportunities for automated support of the reliable operation of the household power system in the event of a high load.

In addition, existing Smart Home systems in most cases require additional network equipment, such as gateways, routers, etc., which introduces additional vulnerabilities and reduces reliability.

It is necessary to ensure the balance of electricity generation and consumption, and for this to do this, it is necessary to be able to monitor the status of consumers and generators and to switch them switching them if necessary. Such a system should be wireless, protected from room interference and unwanted external interference, reliable, and energy-efficient, have a low cost, and can be controlled from a computer or smartphone.

Existing solutions. Smart home communication protocols. A smart home [4] (Digital House, Home Automation) is a house or commercial premises (shop, office, any institution), where electrical appliances are functionally interconnected. They can be connected to a computer network, which allows them to be controlled via a PC and provides remote access to them via the Internet. Thanks to the integration of information technology into the home, all systems and devices coordinate their functions by comparing predefined programs and external indicators. A smart home is created with the help of professional design and programming by companies that develop smart-home projects. The programs entered into the multi-room smart home algorithms are designed to meet the specific needs of residents and situations related to environmental or security changes. A special feature of the smart home is controlled by the remote control, where a person can press a single key to create a certain environment. At the same time, the system itself analyses the surrounding situation and parameters inside the room, and, guided by its conclusions, executes user-defined commands with appropriate settings. In addition, household appliances installed in a smart home can be integrated into a home Universal Plug'n'Play network with Internet access.

The main areas of application of the smart home [5]:

- lighting control systems;
- automated monitoring of the system status: collecting data from various sensors to correct the system status (temperature, humidity, smoke, gas and water leaks, etc.);
- heating, ventilation, and air conditioning systems (HVAC, Heating, ventilation, and air conditioning): remote control of all energy-consuming devices via the Internet using a simple and convenient user interface;
- integration of household appliances with the Smart Grid, for example, to use the electricity generated by solar panels in the middle of the day to run the washing machine;
- a security system integrated with a home automation system can provide additional services, such as remote access to CCTV footage via the Internet, or centralized control of all doors and windows.

However, despite the urgency of the problems being solved and the potential benefits of using smart home technologies, this technology has several significant drawbacks and risks [6]. The main ones are as follows: Internet-connected systems are vulnerable to unauthorized access.

The technology is still in its early stages of development. It is not uncommon for users to invest in systems that are being abandoned by manufacturers. For example, in 2014, Google acquired a company that produced the Revolv Hub home automation system, integrated it with the Nest platform, and in 2016 shut down all the company's servers.

There is a wide range of specialized platforms and protocols designed specifically for building local networks for Smart Home systems. Each of them is essentially a separate language. Each of these languages communicates differently with connected devices and controls them to perform certain functions. These protocols are based on a wired connection, use the power grid, hybrid wireless, or classic wireless. Unfortunately, most of these protocols are not open-source. The main protocols are KNX, Universal Powerline Bus, Zigbee, Z-Wave, and X10.

The main disadvantages of all these communication gaps are the relatively low level of compatibility between different versions, and the need for a gateway with a Wi-Fi network for manual control of the system by the user. A typical integration scheme of such systems is shown in Fig. 1.

In addition to the specialized protocols described above, common technologies such as Wi-Fi or Bluetooth are sometimes used. Their use solves the problem of compatibility and manual system management, and simplifies the system architecture, but poses new challenges to security, power consumption, and reliability. Another important point is the network topologies supported by these protocols, since in urban areas or if the building has thick concrete structures, the most common star topology will have significant limitations in terms of range.

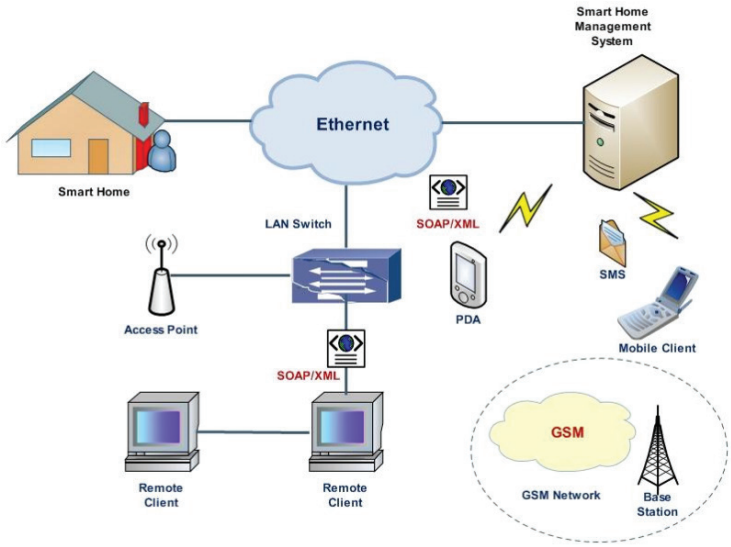

Fig. 1. Typical structure of a Smart Home system

ZigBee protocol. ZigBee [7] is a wireless data transmission standard. It is one of the most popular protocols used in Smart Home systems. It is supported and developed by the ZigBeeTM Alliance of the same name, which was established in 2002 to join forces to develop the most effective protocols and ensure the compatibility of devices from different manufacturers. As the standard improves, the alliance publishes standard specifications, software profiles, and other regulatory documents on its website.

ZigBee is a standard for a set of high-level communication protocols that use small, low-power digital transceivers, based on the IEEE 802.15.4-2006 standard for wireless personal networks, such as wireless headphones connected to mobile phones using shortwave radio waves. The technology is defined by the ZigBee specification, which is designed to be simpler and cheaper than other personal networks such as Bluetooth. ZigBee is designed for mobile devices that require long battery life and secure data transmission in the network.

The system structure of ZigBee technology [8] consists of three main components (Fig. 2): ZigBee coordinator, Router, and end device. Every ZigBee network has to consist of one coordinator which acts as a bridge of the network. The coordinator acts as a hub for receiving and storing important information during the process of transmitting data operations. The ZigBee router acts as an intermediate between the hub of information and end devices which permits the traffic or commands to move through them to the end device.

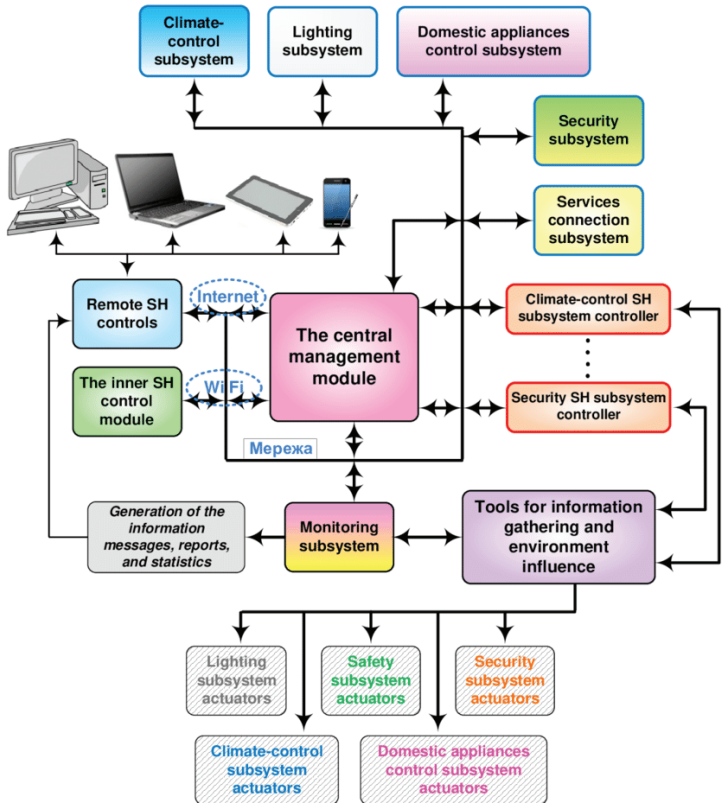

Fig. 2. System structure of ZigBee technology

Advantages:
- low power consumption;
- relatively long range of operation;
- fast recovery from sleep mode (about 3 ms);
- support for various network topologies, including a network that is capable of performing “self-healing” of the network in the event of an of the network.

Disadvantages:
- lack of ZigBee adapters in existing computers, smartphones, etc;
- the need to install expensive adapters on the server or
- creating a gateway between ZigBee and Wi-Fi network;
- insufficiently high level of standardization and a single;
- hardware and software platform for developing complex applications;
- often too slow data transfer speed. Most of the packets;
- is spent on transmitting packets containing address information, synchronization packets, etc. The useful transmission rate is about 30 kbps.

Wi-Fi. Wi-Fi [9] is a commonly used name for the IEEE 802.11 standard for transmitting digital data streams over radio channels. This technology is less commonly used in Smart Home compared to ZigBee, but it has some advantages. Current Wi-Fi implementations allow data transfer speeds of more than 100 Mbps, and users can move between access points within the Wi-Fi network coverage area using devices equipped with Wi-Fi client transceivers and access the Internet. The structure of a conventional Wi-Fi network with Internet access is shown in Fig. 3.

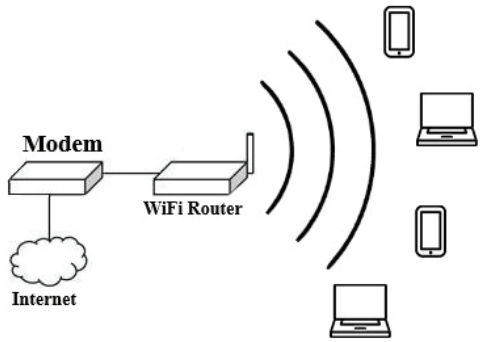

Fig. 3. Block diagram of a typical Wi-Fi network

Typically, a Wi-Fi network layout contains at least one access point and can be easily scaled. It is also possible to connect two clients in the point-to-point (Ad-hoc) mode when the access point is not used, and the clients are connected directly using network adapters.

Wi-Fi Direct technology is a continuation of this trend. Wi-Fi Direct allows computers and portable gadgets to communicate with each other directly via the existing Wi-Fi protocol without using routers and access points. That is, the connection is established

as easily as via Bluetooth. An important point is that to establish a direct connection, it is enough that only one of the devices complies with the Wi-Fi Direct standard. In other words, any modern Wi-Fi-enablement can be connected to certified equipment. The maximum data transmission distance reaches 100 meters.

To summarize, let one formulate the main advantages and disadvantages of using Wi-Fi technology in the field of Smart homes.

Advantages:

– Wi-Fi devices are widespread on the market. Guaranteed compatibility with all devices that have the appropriate adapter;
– The ability of devices to operate in Ad-hoc mode and according to the Wi-Fi direct standard, which does not require a router and modem;
– high level of standardization. Compatibility between devices from different manufacturers.

Disadvantages:

– higher power consumption compared to technologies such as -the impossibility of configuring mesh-topology without additional tools, for this purpose special costly repeaters are used;
– relatively high cost;
– excessive data transmission speed for the needs of Smart Home;
– the range and transmission speed depend only on the power of the router or client adapter.

Bluetooth. Bluetooth [10] is a wireless communication technology created in 1998 by a group of companies: Ericsson, IBM, Intel, Nokia, and Toshiba. In Smart Home, this technology is used less frequently than Wi-Fi and ZigBee, but it has the advantages of low cost, convenient network topology, and high data transfer speed. Currently, Bluetooth developments are being carried out by the Bluetooth SIG (Special Interest Group), which also includes Lucent, Microsoft, and other companies whose activities are related to networking technologies. The main purpose of Bluetooth is to provide power-efficient (in terms of current consumption) and cheap radio communication between various types of electronic devices, such as mobile phones and accessories, laptop and desktop computers, printers, and others.

The Bluetooth interface allows one to transmit both voices (at 64 Kbps) and data. For data transmission, asymmetric (721 Kbps in one direction and 57.6 Kbps in the other) and symmetric (432.6 Kbps in both directions) methods can be used. Operating at a frequency of 2.4 GHz, the transceiver (Bluetooth 26 chip) allows one to establish communication within 10 or 100 meters. The difference in distance is certainly large, but a connection within 10 meters allows for low power consumption, compact size, and fairly low component cost. For example, the low-power transmitter consumes only 0.3 mA in standby mode and an average of 30 mA during information exchange.

Bluetooth technology works on the principle of FHSS (Frequency-hopping spread spectrum). Briefly, this can be explained as follows: the transmitter splits the data into packets and transmits them according to a pseudo-random frequency hopping algorithm (1600 times per second), or a template consisting of 79 sub-frequencies. Only those

devices that are configured for the same transmission pattern can “understand” each other – for third-party devices, the transmitted information will be just noise. The main structural element of the Bluetooth network is the so-called “piconet” - a set of 2 to 8 devices operating on the same pattern. The general scheme of a piconet is shown in Fig. 4.

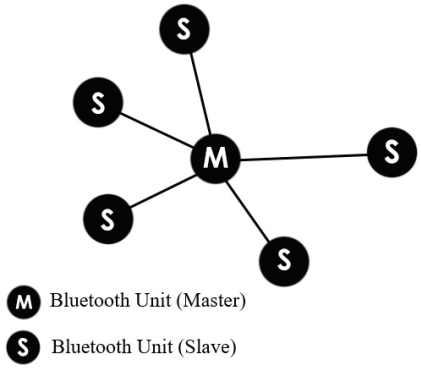

Fig. 4. Bluetooth Piconet network

In each Piconet, one device works as an active (master) and the others as a passive (slave). The active device defines the template on which all the passive devices of its piconet will work and synchronizes its operation. The Bluetooth standard provides for the connection of independent and even non-synchronized peer-to-peer networks (up to 10) into a so-called “scattered”. The general scheme of the “scattered” network is shown in Fig. 5.

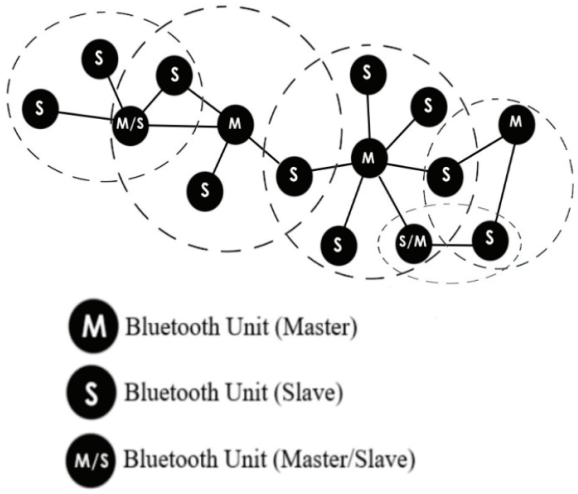

Fig. 5. Bluetooth scatternet network

Initialization, of Bluetooth, is usually called the process of establishing communication. It can be divided into three stages:

– Kinit key generation;
– generation of the communication key (it is called the link key);
– authentication.

The first two steps are part of the so-called pairing procedure. Pairing is the process of connecting two (or more) devices to create a single Kinit secret value. Subsequently, symmetric 128-bit AES encryption is applied to the transmitted data using this key.

To summarize, let's formulate the main advantages and disadvantages of technology Bluetooth.

Advantages:

– high level of standardization;
– reliable data protection system by default;
– a wide variety of Bluetooth modules for different tasks;
– low cost;
– availability of adapters in most gadgets;
– scalable architecture based on the "scattered" principle.

Disadvantages:

– relatively high-power consumption;
– a small range of action;
– lack of mesh topology.

Bluetooth low energy. Low-power Bluetooth or Bluetooth smart is a digital wireless data transmission technology with ultra-low power consumption based on inexpensive chips in transmitting devices. In the field of Smart Homes, this technology was used only a few years ago and in 2017 is one of the most promising areas of IoT and Smart Home development.

Consuming less power, low-power Bluetooth technology offers long-lasting connectivity and connects small devices such as sensors and mobile devices within personal area networks (PANs).

The Bluetooth 4.0 (and later) specification defines two wireless technologies: BR/EDR (classic Bluetooth, which has been evolving since the first version of the standard) and BLE (Bluetooth Low Energy). Devices that use BLE can be either dual-mode BR/EDR/BLE (called Bluetooth Smart Ready), compatible with classic Bluetooth devices, or single-mode BLE (Bluetooth Smart). Features of the structure of these protocols are shown in Fig. 6.

The main blocks of Bluetooth devices are:

– application – implements the logic of work useful for the end user;
– the main device, the host – provides the upper levels of the protocol stack Bluetooth.

It contains the following protocols:

– GAP (Generic Access Profile) – a general access profile;
– GATT (Generic Attribute Profile) – a profile of general attributes;
– ATT (Attribute Protocol) – attribute protocol;

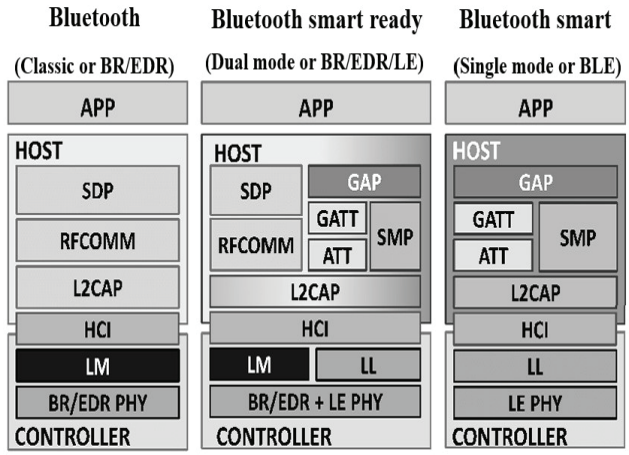

Fig. 6. Scheme of Bluetooth standards

– L2CAP (Logical Link Control and Adaptation Protocol) – a protocol logical link control and adaptation protocol;
– SM (Security Manager) – security manager;
– HCI (Host Controller Interface) – host-controller interface, part of the on the host side;
– Controller – deals with the lower layers of Bluetooth.
Contains protocols:
– HCI – host – controller interface on the controller side;
– LL (Link Layer) – connection level;
– PHY – physical layer.

At the end of 2016, the Bluetooth SIG industry group approved the characteristics of the new Bluetooth 5 standard. The wireless connection range has increased by as much as 400% and the transmission speed has doubled compared to the previous generation of Bluetooth. The updated standard is also more stable and has high security. The main and most anticipated news was the introduction of support for mesh topology, which will significantly increase the size of the network based on Bluetooth Low Energy.

Advantages:
– high level of standardization and compatibility between different protocols;
– low cost;
– ultra-low power consumption;
– the transmission speed of more than 1 Mbps;
– module performance can be customized depending on needs (increasing the transmission speed by reducing the range or vice versa);
– ease of connection;
– communication security;
– availability of unified APIs for working with Bluetooth LE peripherals;

– for most platforms: Android, iOS, and desktop (Java, JS, Python, C++, C#, Ruby, and others).

Disadvantages:

– support for mesh topology appeared only in the latest version 5.0 and is still under active development.

Proposed solutions. One of the most favourable conditions for theft is the New Year holidays. The reason is quite simple, the presence of hosts in the house, because if one want to relax with the whole family and not worry about anything. There are many ways to insure yourself against this, for example: warn your neighbours about your departure and ask them to check your area, a protective film on the windows that will not allow the glass to be broken easily, an alarm, reinforced doors, video surveillance, creating so that in case what to scare intruders [2].

Another danger is the risk of fire and according to the Law of Ukraine [5] it is necessary to follow the rules, and it is better to install smoke sensors to ensure the highest level of protection against fire. According to statistics, the largest number of fires is observed in the residential sector, where 42,381 fires were recorded last year, which is 84% of the total number of fires in the state. Direct losses from these fires amounted to UAH 137.4 million. (28.8%), household – UAH 503.7 million. (45.1%). The main places of fire occurrence in housing are rooms – 9083 (42% of fires in residential buildings), kitchens – 1721 (8%), basements – 1483 (7%), attics – 1432 (7%), coverings and roofs – 1171 (5%) [6].

A comprehensive property protection system is an interconnected set of organizational and engineering measures, means, and methods of property protection [9].

Consider the "smart home" system [10]. Currently, this security system remains the best, and at the same time the most expensive, for a private home.

They require a more complex installation and can print other systems, not just alarms. Systems are typically integrated and individual protection functions can operate autonomously. Complexes may include video surveillance systems, alarms, and motion sensors for private homes. They are equipped with control panels and remote access. Notification methods may also differ. These systems are considered completely autonomous, but owners can connect them to special services. When an alarm signal is received, the appropriate security service will arrive. Here is what happens. If an intrusion is detected, appropriate action will be taken. The main problem of such a system is the extremely high price and payment for the services of healthcare companies.

The leading home security system is high-quality, simple, and inexpensive. Its advantages include the fact that working sensors do not require battery replacement and standard charging. A special unit that provides uninterrupted power must work during a power outage. The sensor and camera must be connected to the system. The set of functions depends on the wishes of the owner.

A wireless security system is safe for a private home since there are no wires in it. No need to spend on maintenance to install such equipment. They are ideal for a private home and office. A private GSM home security system has many features. Sensors or IP cameras work together with the control unit via Wi-Fi or radio frequency. In case of danger, an SMS is sent to the phone number registered in the system. But there were more such devices than wires.

For the security system to optimally perform its work, it is necessary to pay attention to its selection. A few rules for this:

1) it is not worth saving, after that it can have a bad effect on reliability;

2) it is better to contact the security organization in advance, this will allow them to calculate where the system will be placed;

3) a consultant can help with the choice;

4) installation should be done by professionals since it is impossible to do it well without special knowledge.

If a company has been selected, experts will recommend equipment and map the site and potential hazards. It is also necessary to install the necessary alarm response function. If the threat is reported only to the owner, likely emergency measures will not be taken. It is desirable that the company also follows this [10]. Security companies sell and install equipment. They also perform maintenance. Employees choose the appropriate system for the product for added security. For the device to always work well, one should check it regularly. And the right action will save a lot of trouble. It is important to have a plan in place to notify helpers in an emergency. The operation of this installation must be constantly checked, but this must be done by specialists. It is necessary to monitor changes in the field of security, to improve their equipment with the help of new functions. A built-in alarm with radio and wired channels can be used, making it difficult to penetrate the facility or service area.

The equipment itself requires maintenance, and security systems are no exception. This will allow the timely detection of the most vulnerable places and their elimination. Testing extends the life of the device. Maintenance includes the elimination of defects and replacement of equipment or its parts. Tests are required to diagnose the operation and visual inspection. Experts monitor the state of regulators, indicators, and other details. A thorough inspection ensures the smooth operation of the equipment. And if this work is not done often, then the sensors may act incorrectly or give false results. If equipment fails, it must be repaired or replaced. A security alarm system is reliable for home security. All one have to do is choose the right option and then order the job.

The cost of a security system is determined by many factors. More options – more price. For example, if the security of the house or only the territory was ordered impersonally, the cost will be minimal. The most expensive option is to order a set of devices that includes all protection functions. But, such a system is considered the best, as it provides reliable protection.

Another way to ensure security is the alarm system, which allows one to monitor and notify about the following processes taking place in the object under protection:

- destruction of windows, walls, and ceilings;
- opening doors and windows;
- movement of people inside the premises.

Many homeowners choose video surveillance. This equipment is also a security system. This allows one to monitor the house and surrounding areas in real time. Materials are usually saved so that they can be viewed. There are two types of home security systems: analogue and digital. The second type of video surveillance is considered the

best. Since the device is created on the basis of modern technologies, the performance will be better. Digital video surveillance has certain advantages:

- available control from a computer, tablet, or phone;
- a wide selection of tools with different functions;
- connection for image analysis;
- access control;
- automatic system verification process;
- quick installation.

In addition, this method provides the user with a constant opportunity to monitor the situation in the protected area with the help of an application on a smartphone. We implemented a video surveillance system that allows the user to manage, configure and receive information from video surveillance cameras through a smartphone, or rather through the Telegram messenger. This method is chosen due to its convenience and reliability. Telegram is known for its level of protection and refusal to share users' personal data. It is also extremely easy to master. The work of this program is implemented with the help of commands, by entering which, the user can get the information he needs. These commands can be changed for each user, which provides system variability for each user.

Conclusion. The principles of operation of such systems, both autonomous and human-controlled, are analysed. Methods of communication with systems of this type by cable or remotely are considered, depending on the ease of use. In addition, the systems are analysed in their specification, i.e. what exactly they protect, such as systems for protection against intrusion into the house and theft, as well as systems that control fire safety, gas leakage, etc. When considering such systems, their weaknesses, and strengths are taken into account in order to choose the best option.

The methods of construction and implementation of protection systems, what is needed for them, and the advantages of certain means of implementation are studied. Various hardware specifications and related tools for its operation, such as power supply and installation requirements are analysed.

The expediency of the development in the field of defence is considered, the prospects of this development are evaluated and substantiated, and its improvements in the future are described.

The developed program is presented, its functionality is described, and the expediency of this development is justified.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bluetooth Low Energy. URL: https://novelbits.io/bluetooth-low-energy-ble-complete-guide (Accessed: 29/01/2023).
2. Smart dispatcher. URL: https://hytera-europe.com/news/what-is-smart-dispatch (Accessed: 29/01/2023).
3. Зелена книга. Регулювання роздрібного ринку електричної енергії. URL: https://cdn.regulation.gov.ua/12/ed/8b/5a/regulation.gov.ua_GP%20Electricity%20market.pdf (Accessed: 29/01/2023).

4. Smart Home. URL: https://uk.wikipedia.org/wiki/Розумний_дім (Accessed: 29/01/2023).
5. Areas of application. URL: https://www.techtarget.com/iotagenda/definition/smart-home-app-home-automation-app (Accessed: 30/01/2023).
6. Уразливості в системах «розумного дому» дозволяють хакерам Вас підслуховувати. URL: https://cybercalm.org/novyny/urazlyvosti-v-systemah-rozumnogo-domu-dozvlyayut-hakeram-vas-pidsluhovuvaty/ (Accessed: 30/01/2023).
7. ZigBee protocol. URL: https://www.geeksforgeeks.org/introduction-of-zigbee/ (Accessed: 30/01/2023).
8. Wi-Fi: IEEE 802.11. URL: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/what-is-wifi.php (Accessed: 30/01/2023).
9. Технологія бездротового зв'язку малого радіусу дії проти технології бездротового зв'язку великого радіусу дії. URL: https://www.mokosmart.com/uk/short-range-wireless-communication-technology-vs-long-range-wireless-communication-technology/ (Accessed: 30/01/2023).
10. Data Sheet Bluetooth Low Energy Module RN4020. URL: https://ww1.microchip.com/downloads/en/DeviceDoc/50002279B.pdf (Accessed: 30/01/2023).

REFERENCES

1. Bluetooth Low Energy. Retrieved from https://novelbits.io/bluetooth-low-energy-ble-complete-guide (Accessed: 29/01/2023) (in English).
2. Smart dispatcher. Retrieved from https://hytera-europe.com/news/what-is-smart-dispatch (Accessed: 29/01/2023) (in English).
3. Zelena knyha. Rehuliuvannia rozdribnoho rynku elektrychnoi enerhii. Retrieved from https://cdn.regulation.gov.ua/12/ed/8b/5a/regulation.gov.ua_GP%20Electricity%20market.pdf (Accessed: 29/01/2023) (in Ukrainian).
4. Smart Home. Retrieved from https://uk.wikipedia.org/wiki/Rozumnyi_dim (Accessed: 29/01/2023) (in English).
5. Areas of application. Retrieved from https://www.techtarget.com/iotagenda/definition/smart-home-app-home-automation-app (Accessed: 30/01/2023) (in English).
6. Urazlyvosti v systemakh «rozumnoho domu» dozvoliaiut khakeram Vas pidslukhovuvaty. Retrieved from https://cybercalm.org/novyny/urazlyvosti-v-systemah-rozumnogo-domu-dozvlyayut-hakeram-vas-pidsluhovuvaty/ (Accessed: 30/01/2023) (in Ukrainian).
7. ZigBee protocol. Retrieved from https://www.geeksforgeeks.org/introduction-of-zigbee/ (Accessed: 30/01/2023) (in English).
8. Wi-Fi: IEEE 802.11. Retrieved from https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/what-is-wifi.php (Accessed: 30/01/2023) (in English).
9. Tekhnolohiia bezdrotovoho zv'iazku maloho radiusu dii proty tekhnolohii bezdrotovoho zv'iazku velykoho radiusu dii. Retrieved from https://www.mokosmart.com/uk/short-range-wireless-communication-technology-vs-long-range-wireless-communication-technology/ (Accessed: 30/01/2023) (in Ukrainian).
10. Data Sheet Bluetooth Low Energy Module RN4020. Retrieved from https://ww1.microchip.com/downloads/en/DeviceDoc/50002279B.pdf (Accessed: 30/01/2023) (in English).

doi: 10.32403/1998-6912-2023-2-67-120-135

ДОСЛІДЖЕННЯ ТА ПРОЄКТУВАННЯ АВТОМАТИЗОВАНОЇ БАГАТОФУНКЦІОНАЛЬНОЇ СИСТЕМИ ДЛЯ ТЕХНОЛОГІЇ «РОЗУМНИЙ БУДИНОК»

С. І. Гапій[1], Р. Л. Ткачук[2]

[1]Національний університет «Львівська політехніка», вул. С. Бандери, 12, Львів, 79013, Україна

[2]Львівський державний університет безпеки життєдіяльності, вул. Клепарівська, 35, Львів, 79007, Україна
serhii.hapii.mkiks.2022@lpnu.ua,
rlvtk@ukr.net

Однією з основних функцій системи «Розумний будинок» є забезпечення безпеки та цілісності різних типів об'єктів (будівель, прилеглих територій, окремих приміщень, різних видів транспорту тощо). Встановлено, що основними умовами ефективності систем безпеки є індивідуальний вибір оптимального комплекту датчиків та їх коректна інсталяція. Також основою ефективності роботи цих систем є високофункціональність та швидке реагування на різноманітні виклики.

Крім того існуючі системи «Розумний дім» у більшості випадків вимагають додаткового мережевого обладнання, такого як шлюзи, маршрутизатори тощо, що створює додаткові вразливості та знижує надійність. Тому виходячи з цього надійна система має бути бездротовою, захищеною від перешкод із приміщення та небажаного зовнішнього втручання, енергоефективною, мати невисоку вартість можливість дистанційного керування з комп'ютера чи смартфона.

У статті проведений аналіз принципів роботи як автономних, так і керованих людиною систем. Розглянуто способи зв›язку з системами такого типу по кабелю чи дистанційно в залежності від зручності використання. Також наводяться результати проведеного аналізу систем в їхній специфікації, тобто що саме вони захищають, наприклад системи захисту від проникнення в будинок і крадіжки, а також системи контролю пожежної безпеки, витоку газу і т.д. Досліджено способи побудови та реалізації систем захисту, визначено необхідні компоненти та переваги окремих засобів реалізації. Проаналізовано різні специфікації апаратного забезпечення та пов'язані інструменти для її роботи, наприклад вимоги до джерела живлення та інсталяції.

Розглянуто доцільність розробки у сфері забезпечення захисту, оцінено та обґрунтовано перспективи пропонованої розробки, описані її можливості щодо масштабування та вдосконалення у майбутньому.

Обраний спосіб реалізації системи надає користувачеві постійну можливість стежити за подіями на об'єкті який охороняється, використовуючи для цього

програмне забезпечення на смартфоні. Також нами була запропонована та впроваджена система відеоспостереження, яка дозволяє користувачеві керувати, налаштовувати та отримувати інформацію з камер відеоспостереження через смартфон, а точніше через месенджер Telegram. Цей спосіб був обраний через його зручність і надійність оскільки Telegram канал має високий рівень захисту та використовує політики які забороняють передавати особисті дані користувачів третім особам. Робота цієї програми реалізується за допомогою команд, ввівши які, користувач може отримати необхідну йому інформацію. Ці команди можна змінювати для кожного користувача, що забезпечує високий рівень адаптивності самої системи до вимог та потреб кожного користувача.

В статті наведено розроблену програму, описано її функціональні можливості та обґрунтовано доцільність цієї розробки.

Ключові слова: *кіберзахист, система безпеки, датчики, оповіщення, охорона.*

Стаття надійшла до редакції 26.06.2023.
Received 26.06.2023.