N. Shkoliar, PhD in Ped., As. Prof.
N. Kupchyk, Student
Khmelnytskyi National University

ANALYSIS OF SMART HOME SECURITY METHODS

The aim of the research was to analyze and investigate the methods of securing a smart home system. Based on this study, data was obtained from various sources.

Comfort is the first concept that comes to mind for modern individuals when choosing their own living space. With each passing day, information technologies are evolving more and more, and today, few people are surprised by “smart” household appliances and other technological capabilities. Relatively recently, the term “smart home” has appeared in human usage.

A smart home is a home in which devices are connected, can be customized, programmed, and controlled remotely using a smartphone or computer [1].

Advantages of using a smart home system include the following:

- increased security level;
- optimization of energy consumption;
- convenience and comfort;
- entertainment and relaxation opportunities [2].

Disadvantages of the smart home system are:

- dependence on the internet and electricity;
- privacy and cybersecurity issues;
- high standards and device compatibility requirements;
- high installation costs;
- need for specialized maintenance [3].

By utilizing smart home technologies and having constant access to the internet and electricity, various processes can be configured according to the needs of each family member. Additionally, the security level can be increased. Devices such as surveillance cameras, smoke detectors, water sensors, and alarms can quickly alert homeowners to dangers in the home and allow remote management of security systems. However, such complete dependence on the internet can limit or completely impair functionality, and it also increases vulnerability to cyberattacks and the loss of personal data and control systems. It is not possible to fully protect a smart home system, but measures can be taken to make it more difficult for attackers to compromise.

Among such methods, the following can be highlighted:

- network segmentation;
- strong passwords;
- two-factor authentication;
- data encryption;
- firmware updates;
- device isolation;
- intrusion detection with specialized hardware or software;
- physical security;
- user education.

Performing network segmentation and device isolation can increase the security level of devices, prevent unauthorized access to devices, and limit the damage caused by compromised devices. However, it should be noted that these methods can be complex to configure and may partially restrict the functionality of devices. Using strong passwords and two-factor authentication can also prevent unauthorized access to devices, although these methods may be inconvenient for users, they are effective because an attacker would need to find other ways to crack passwords and bypass the additional security layer. Data encryption is also an effective method of protecting confidential data from unauthorized access, but it should be noted that such a method may slow down performance. Firmware updates allow users to address existing vulnerabilities and errors in security and improve the functionality of devices. In order to ensure that users do not forget to update the firmware, it is advisable to set reminders or, if possible, enable auto-updates. However, it should be noted that some updates may cause network failures, and this should also be taken into account and problems should be addressed promptly. Using devices such as smart locks, surveillance cameras, motion sensors, and other devices can help homeowners detect potential threats. Using specialized anomaly detection software, such as Suricata, Snort, Bro IDS, etc., can help analyze network traffic and detect threats in real-time. These tools are equally effective, but they can be expensive to set up and maintain. Another important method is user education to prevent common mistakes and maintain security and confidentiality, including users implementing methods such as using strong passwords and two-factor authentication [5]. Combining the above-described options into a unified complex will help enhance the security level of the smart home system. However, it is worth considering that the use of the methods described above will not protect the system by one hundred percent, but it will definitely complicate the hacking process.

REFERENCES

1. What is a Smart Home? [Електронний ресурс] https://smarthomeenergy.co.uk/what-smart-home/

2. Можливості розумного будинку – огляд системи. [Електронний ресурс] https://vencon.ua/ua/articles/vozmozhnosti-umnogo-doma-obzor-sistem

3. Розумний будинок: переваги та недоліки. [Електронний ресурс] https://buduemo.com/ua/news/smart_systems/what-is-a-smart-home.html

4. Як захистити «розумний будинок» від злому? [Електронний ресурс] https://worldvision.com.ua/kak-zashchitit-umnyy-dom-ot-vzloma/

5. Choudhary, Y., Umamaheswari, B., Kumawat, V. A study of threats, vulnerabilities and countermeasures: An IoT perspective. / Shanlax International Journal of Arts, Science and Humanities. vol. 8, no. 4, 2021, pp. 39-45.