УДК 004.057.4

Kolomatska D.S. student of group 125-22-3
(Dnipro University of technology, Dnipro, Ukraine)

SOLVING SECURITY ISSUES IN IOT SYSTEMS

IoT is a network concept that plays one of the key roles in today's technological environment, providing the ability to connect devices, allowing the exchange of data.

Thanks to artificial intelligence and pre-programmed decisions, machines can make autonomous decisions without human intervention. This feature helps improve performance and reduce event response time. An example is the "Smart House" figure 1. "Smart House", like all other Internet IoT things, greatly simplifies human life. For example, having a house with this function, we can program the air temperature, turning on the light, turning on the kettle while being far from the house.

Wide implementation of such systems takes place in the organization of automated heating and air conditioning control systems in the "smart house" [1-3]. The application of such systems also takes place in the orientation [4]. Algorithms for decision-making are described in [5].

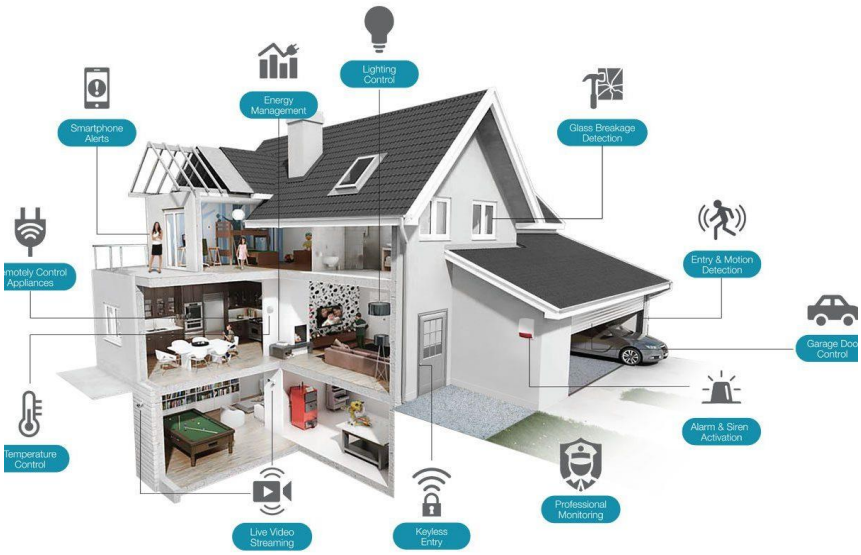

Figure 1 – a visual scheme of the "Smart House" system

But despite all the conveniences of the IoT system, there are many security issues:

- high initial costs;
- installation and maintenance;
- user safety;
- compatibility of systems.

The first question arises because of significant financial costs. Installation of video cameras, sensors, program development, hardware and control systems are beyond the reach of people with an average income. The solution will be the provision of subsidies, tax and government programs for small businesses and enterprises. Or the option to rent IoT equipment, which reduces the high initial costs.

The second issue arises due to the fact that the equipment requires adjustment, constant technical support and timely updates. All this increases costs and effort. The solution to this issue will be an intuitive interface and service automation. Therefore, a simple and user-friendly interface will be understandable to users who do not have special technical skills or knowledge, which significantly reduces maintenance costs. Also, using a system with

automatic software updates and self-calibrating sensors can reduce the need for regular system intervention.

The third issue is user security. If IoT elements are not properly protected from tampering with robust algorithms, such systems will do more harm than good, providing cybercriminals with a loophole to undermine information security. Since things with built-in computers store a lot of information about their owner, in particular, they can know their exact location. To ensure security, it is necessary to develop standardized solutions using reliable encryption methods that will guarantee the protection of data from intruders.

The last problem, in my opinion, is the compatibility of the system. During the implementation of the project, there may be a resonance of systems with the integration of equipment from several manufacturers using different standards and protocols. The solution to the problem will be the use of open protocols and standards, the choice of equipment from those manufacturers that offer support for many standards, protocols and guarantees of compatibility with other devices.

REFERENCE

1. Олішевський, І. Г. (2015). Justification rational scheme of heat pump system heating. MECHANICS OF GYROSCOPIC SYSTEMS, (30), 26. https://doi.org/10.20535/0203-377130201573171

2. OLISHEVSKYI I.H. Automated methodology of calculating parameters for non-traditional technology of heating mode of hydro-storage power plant station / OLISHEVSKYI I.H., GUSEV O.YU., OLISHEVSKYI H.S. // Електротехніка та електроенергетика. / Запорізький нац. ун-т «Запорізька політехніка». – Запоріжжя, 2023. – № 1. – С. 36-42. https://doi.org/10.15588/1607-6761-2023-1-4

3. OLISHEVSKYI I.H. (2024). RESULTS OF DEVELOPMENT AND RESEARCH OF THE TECHNOLOGY FOR AUTOMATED ENERGY-EFFICIENT CONTROL OF HEAT PUMP SYSTEMS BY MEANS OF COMPUTER EXPERIMENT. Herald of Khmelnytskyi National University. Technical Sciences, 335(3(1), 419-428. https://doi.org/10.31891/2307-5732-2024-335-3-58

4. Pivnyak, G., Olishevska, V., Olishevskiy, H., Lutsenko, I., Lysenko, A., & Sala, D. (2024). Comprehensive study on electric vehicles and infrastructure for sustainable development in Ukraine. E3S Web of Conferences, 567, 01025. https://doi.org/10.1051/e3sconf/202456701025

5. Khabarlak, K. S. (2022). FASTER OPTIMIZATION-BASED META-LEARNING ADAPTATION PHASE. Radio Electronics, Computer Science, Control, (1), 82. https://doi.org/10.15588/1607-3274-2022-1-10