нових способів взаємодії між учасниками, додавання та підтримку різних мов, оскільки проблеми кіберзахисту є проблемами суспільства вцілому.

Список використаних джерел

1. 8 инструментов для моделирования кибератак для повышения безопасности [Електронний ресурс]. – Режим доступу до ресурсу: https://itsecforu.ru/2018/12/11/8-инструментов-моделирования-киберат/

2. Приниятие решений в условия частичной неопределенности [Електронний ресурс]. – Режим доступу до ресурсу: https://studbooks.net/29425/ekonomika/prinyatie_resheniy_usloviyah_chastichnoy_neopredelennosti.

3. Вирус Petya в Украине: Британия официально обвинила Россию [Електронний ресурс]. – Режим доступу до ресурсу: https://fakty.com.ua/ru/svit/20180215-virus-petya-v-ukrayini-brytaniya-ofitsijno-zvynuvatyla-rosiyu/

4. Грабовый А. Закон о кибербезопасности и стратегия кибербезопасности Украины [Електронний ресурс]. – Режим доступу до ресурсу: http://uz.ligazakon.ua/magazine_article/EA010553

5. Защита киберпространства в разных странах [Електронний ресурс]. – Режим доступу до ресурсу: http://www.inf74.ru/safety/ofitsialno/zashhita-kiberprostranstva-v-raznyih-stranah/

UDC 004.738.5 : 004.77

ADVANTAGES AND DISADVANTAGES OF INTRODUCING IOT DEVICES

Skliarova D.Y., student the group CE-162 ,
Svetenok L.K., senior lecturer
Chernihiv National University of Technology (Chernihiv, Ukraine)

The Internet of Things (IoT) is a network concept consisting of interconnected physical devices that have embedded sensors as well as software that allows transmission and exchange of data between the physical world and computer systems by means of standard communication protocols. In addition to the sensors, the network may have actuators built in physical objects and interconnected via wired or wireless networks.

The main concept of IoT is the ability to connect all kinds of objects (things) that people can use in their everyday life, such as refrigerators, air conditioners, cars, bikes and even sneakers. All these objects (things) have to be equipped with built-in sensors capable of processing the information received from the environment, exchanging it and performing various actions depending on the information received. [1].

According to Statista, over 23.14 billion devices are connected worldwide using IoT technology. Figure 1 shows the number of connected devices (IoT) worldwide from 2015 to 2025. By 2020, the installed base of IoT devices is forecast to have reached almost 31 billion worldwide. [2]
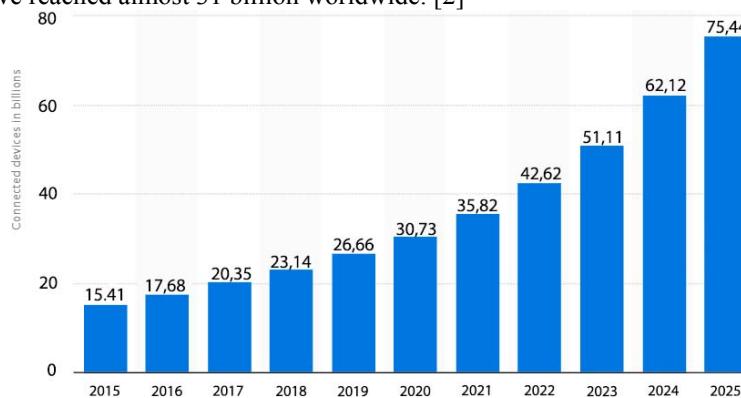

Figure 1. The statistics of connected IoT devices

3 ways of interaction with the Internet things are direct access, access through gateway and access via server.

In the case of direct access Internet things must have their own IP addresses or network alias, accessible from any client application and they must perform the functions of a web server. The interface with such things usually looks like a web resource with a graphical interface controlled by a web browser.

If Internet things do not have built-in support for IP and HTTP protocols, but support private protocols, such as Bluetooth or ZigBee, a special Internet gateway can be used to interact with them.

The third form of interaction of devices in IoT via server implies the presence of an intermediary between Internet things and a user and can be implemented with the aid of an intermediary data platform. This approach assumes the presence of a centralized server or a group of servers the main functions of which include receiving messages from the Internet of things and transferring them to users, storing and processing the received information and providing a user interface with the possibility of two-way exchange between the user and the Internet thing.

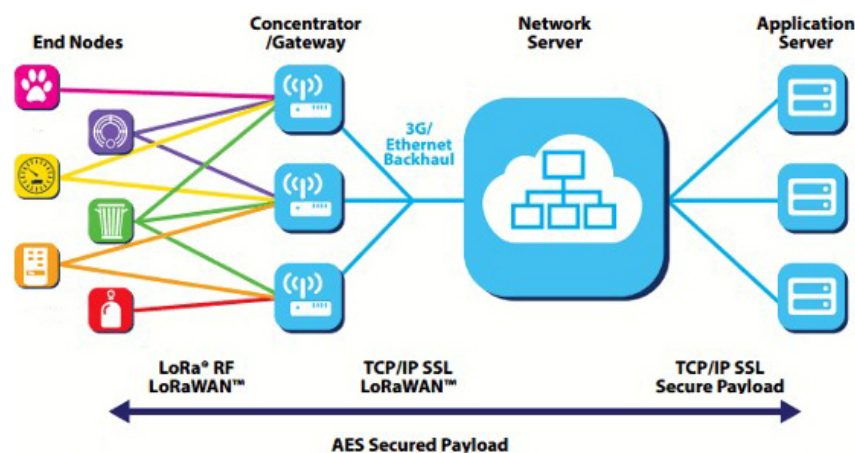A complete system of interaction is displayed in figure 2.

Figure 2. Types of interaction with Internet things

The advantages of using IoT devices are following:

Communication. IoT encourages the communication between devices, also famously known as Machine-to-Machine (M2M) communication. Because of this, the physical devices are able to stay connected and hence the total transparency is available with lesser inefficiencies and greater quality.

Automation and Control. Due to physical objects getting connected and controlled digitally and centrally with wireless infrastructure, there is a large amount of automation and control in the workings. Without human intervention, the machines are able to communicate with each other leading to faster and timely output.

Information. It is obvious that having more information helps making better decisions. Whether it is mundane decisions as needing to know what to buy at the grocery store or if your company has enough widgets and supplies, knowledge is power and more knowledge is better.

Monitor. One more most obvious advantage of IoT is monitoring. Knowing the exact quantity of supplies or the air quality in your home, can further provide more information that could not have previously been collected easily. For instance, knowing that you are low on milk or printer ink could save you another trip to the store in the near future. Furthermore, monitoring the expiration of products can and will improve safety.

Time. As hinted in the previous examples, the amount of time saved because of IoT could be quite large. And in today's modern life, we all could use more time.

Money. The biggest advantage of IoT is saving money. If the price of the tagging and monitoring equipment is less than the amount of money saved, then the Internet of Things will be very widely adopted. IoT fundamentally proves to be very helpful to people in their daily routines by making the appliances communicate to each other in an effective manner thereby saving and conserving energy and cost.

The disadvantages of using IoT devices are following:

Compatibility. Currently, there is no international standard of compatibility for the tagging and monitoring equipment. This disadvantage is believed to be one of the easiest to overcome. The manufacturing companies of such equipment just need to agree to a standard, such as Bluetooth, USB, etc.

Complexity. As with all complex systems, with IoT there are higher risks of failure. For instance, if two users sharing one device each get a message saying that something has expired, both can stop at a store on their way home and purchase it. As a result, there will be double amount purchased. Moreover, there might be a software bug, which will end up in ordering a new ink cartridge for the printer automatically after each power failure, when only a single replacement is needed.

Privacy/Security. As far as a lot of IoT data are transmitted the risk of losing privacy increases. Users do not usually know how well encrypted the data are kept and transmitted with. In addition they do not want to share their sensitive data with anybody.

Safety. Safety is ultimately in the hands of the consumer to verify automation. It will make impossible such situations as automatic shipment of an equivalent product that a user can be allergic to, or a flavor that they do not like, etc. [3]

As it can be seen the using of IoT has more advantages than disadvantages. Though like any rapidly developing technology IoT is experiencing a number of so called "growth diseases". The most serious of them is the problem of security as the bigger amount of "smart" devices connect to the network, the higher are risks associated with unauthorized access to an IoT-system and use of its capabilities by intruders. But nowadays, the efforts of many IT companies and organizations are aimed at finding solutions that will minimize the threats that hinder full implementation of IoT so we believe that future of IoT is promising.

References
1. Інтернет речей [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Інтернет_речей
2. Статистика інтернету речей [Електронний ресурс]. – Режим доступу: https://www.statista.com
3. Pros & Cons of Internet Of Things [Електронний ресурс]. – Режим доступу: https://habr.com/ru/company/unet/blog/410849/