4. Інформаційний бюлетень СФД (дайджест). НІІ мікрографії. Випуск № 06(118) 2014. – 39 с. Режим доступу: http://micrography.gov.ua/index.php/ru/digest

5. «Сохранение электронного контента в России и за рубежом». Сборник материалов Всероссийской научной конференции. (Москва, 24–25 мая 2012 г.). – 151 с. – Режим доступа: http://www.programma.x-pdf.ru/16kulturologiya/550090-2-sohranenie-elektronnogo-kontenta-rossii-rubezhom-sbornik-materialov-vserossiyskoy-konferencii-moskva-24-25-maya-2012.php

6. Запровадження стандартів ISO 14721:2012 та ISO 16363:2012 у Чехії. – Режим доступу: http://rusrim.blogspot.com/2014/09/iso-147212012.html

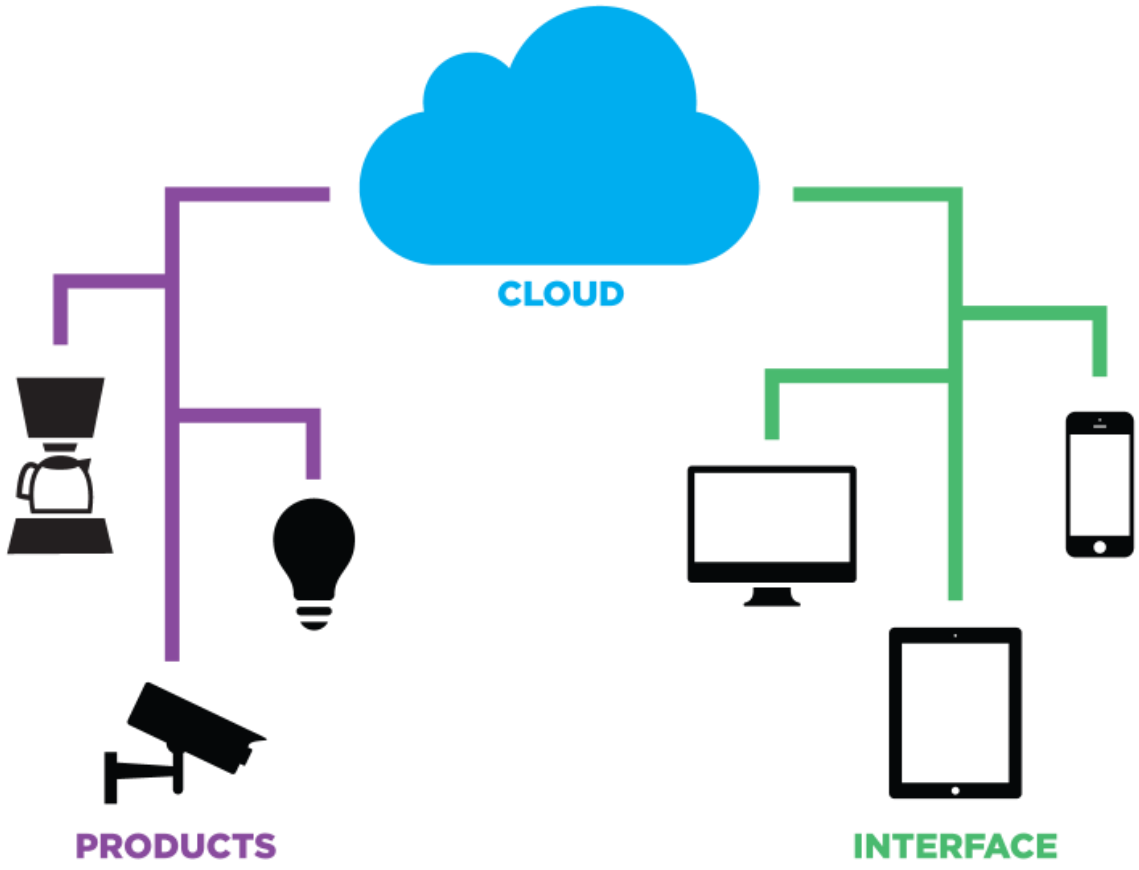
Shatohina A.S.
Student,
Kharkiv Scientific-Reserch Institute of Banking

SECURITY OF THE INTERNET OF THINGS

Internet of things is one of which will develop innovations in wireless, mobile and cloud technologies. It helps to integrate all devices having means of communication into one network than helps greatly simplify our lives. Most often the notion of Internet of things is inextricably linked with something smart: smart houses, smart transport, smart companies... However, for corporations «joint universe» carries not only the undeniable advantages, but various difficulties, including those related to security.

Despite all the talk, which are now about the Internet of things, nobody came to the consensus that the same is itself IoT and that under this expression to understand. «The first big problem is that different organizations have different understanding what is the Internet of things,» said Gartner analyst Earl Perkins.

Under a particular organization understands the essence of what the Internet of things, directly depends on its goals and objectives in the use of the Internet of things. How could anyone not understand and for what purposes did not use IoT, there will always be a certain foundation on which stands the Internet of things. Without which it is impossible to arrange such a complex unified infrastructure. 451 Research company researcher Brian Partridge says that this foundation consists of «devices, networks and a cloud service».



And on each of the components of the Internet of things, there is a problem of security and they are sure to arise if the system beforehand is designed incorrectly. Internet of things implies the existence of links between many elements, which seriously complicates the infrastructure, because the more complicated mechanism, the more chance of breakage, IB expert company LIFARS Ondrej Krehel says that this leads to problems («complexity is the main enemy of security») in our case hacking and loss of valuable information, and for large banks and companies, this means a huge financial loss. After all, nowadays a large number of smartphones, which are not inferior to the technical component of modern computers, and is easy for hackers to hack someone account with lots of zeros. Among the new types of devices now popular smart watch, fitness bracelets and other portable device that resembles the head of the team of consultants at Check Point Software Technologies (produces network security equipment) Anton Razumov. From the point of view of

information security at clever hours vulnerable encrypted communication channels. He knows that there are special attacks that allow you to decipher the information and get access to the personal data of the user watch. During this process, the iOS or Android device-is not important, said Razumov.

In the case of many devices that collect information such as your name, address, data of birth, medical information and credit card numbers, privacy concerns and security are compounded by the fact that along with them work cloud services and mobile applications.

Now, there are basic safety equipment for industrial systems smart homes, energy, petrochemistry, Khayretdinov notes. On the safety of domestic Internet of things should take care of the manufacturer, and not the user that is unlikely to do something for the sake of his defence, he reasons. According to Khayretdinov, you should see a special controller, which would establish security requirements and vendor attracted special protective producers would decisions and even insurance companies. For appliances of such regulator now in Ukraine or abroad, said Khayretdinov.

There are lots of basic security controls that can significantly raise the level of security. Many of the vulnerabilities identified in the framework of this study, are relatively easy to fix and do not affect the user experience. Security is a process, stretched over the entire life cycle of the product, because no matter how many new remedies would avoid the new method can always be found their hacking.

The era of interconnected smart devices have already occurred, though is in the early stages. Gartner predicts that by the year 2020, the number of devices on the Internet of things will be 26 billion units. Fortunately, there is still time to take care of security issues before consumers would face a risk, because the technologies never stand still.

References:

1. Как интернет вещей меняет подход к безопасности в корпорациях перевод https://habrahabr.ru/company/1cloud/blog/254505/

2. Интернет вещей открывает киберпреступникам новое поле деятельности https://www.vedomosti.ru/technology/articles/2016/02/29/631753-internet-veschei-otkrivaet-kiberprestupnikam-novoe-pole-deyatelnosti

3. Умный интернет вещей – кто он и с чем его едят? https://habrahabr.ru/post/259243/