means the end of the relationship. However, the Internet has made the process much easier.

4. Ability to make money on the Internet.
5. Strengthening self-esteem.
6. Ability to learn foreign languages on your own.

Conclusion. So, having considered some investigations on the topic we may conclude that benefits or disadvantages of the Internet entirely depend on how the person uses it.

References:

1. Інтернет – користь чи шкода [Electronic resource]. – Access mode: http://molodi.in.ua/itkoryst/
2. Інтернет [Electronic resource]. – Access mode: https://uk.wikipedia.org/wiki.

Roman Dolinovski
Research supervisor: Mykhailo Kasianchuk
Candidate of Sciences in Physics and Mathematics, Associate Professor
Language tutor: Lilia Shtokhman,
Candidate of Philological Sciences, Associate Professor
Ternopil National Economic University

FINGERPRINT AND IRIS SCANNER

At present, the protection of information in the IT universe is an important issue. There are plenty of ways to do this. Fingerprint scanner and iris scanner are considered to be the best technologies of protecting your information.

So, the aim of our research is to present the topic about scanners helping us to save information.

The fingerprint scanner uses the individual fingerprint of each person. Only the retina scanner, as professionals admit, can be better [1]. The first company that installed such a device in its smartphone was Apple. It was IPhone 5s that first incorporated such a data protection device. After this all pocket gadgets developers began installing these trend add-ons into their inventions [2].

There are three types of fingerprint scanner: optical, semiconductor, and ultrasound. We will consider only the optical type because it is installed in most modern gadgets. It seems that this is a complicated mechanism that uses a heat sensor or can scan the relief. In fact, it works like a usual camera with the special software matching two images [1].

But, as the producers say, using a fingerprint scanner on a smartphone, tablet personal computer, laptop or other electronic devices isn't so safe. Not so long ago specialists from two universities created a so-called image of a "universal fingerprint". In this picture there are a huge number of different people's prints and signs. Experiments have shown that this imprint is enough to cheat most of the inexpensive scanners installed in mobile phones, tablets, laptops and other electronics [2].

The introduction of the iris scanner into smartphones began in 2015. These were the Chinese and Japanese developers who installed it first. In particular, the pioneer was ViewSonic V55, which never was launched into sale. Samsung Galaxy S8 was the newest smartphone with this scanner, but it was easily deceived by hackers who printed a photo on a printer and put a contact lens on it.

Irrigation scanner technology is recognized as one of the most secure forms of biometric authentication since the iris pattern is impossible to reproduce. According to the theory of probability, there have not yet been two people in the whole history of mankind who would have had a matching eye pattern. The iris scanner is often mistakenly called the retina scanner. The difference is that the retina is located inside the eye and cannot be scanned with an optical sensor, only with the help of infrared radiation [1].

The principles of its functioning are similar to the fingerprint scanner, but it uses the software that is more complex – a monochrome camera with a dim backlight, sensitive to infrared radiation allowing to work in low light conditions. Usually a series of several photographs is made, since the mechanism is sensitive to light and constantly changes its size. Then software picks the best photo, determines the borders of the iris and the control area, applies special filters to each point of the selected area to extract phase information and converts the shell pattern into a digital format. The iris scanner is about 10 times more accurate than fingerprint scanning [1].

The specialists say that this system will be able to operate in wider areas, for example, in a smart house, access control systems, or in ATMs. All these devices will be able to exchange information with each other from a single database, where the irises of family members, company employees or citizens of the country are stored. However, the disadvantage of this technology is its price [1].

Conclusion. So, as we have seen there are several devices for storing data, but there are ways to cheat them. You cannot be sure of them, just like of any other security means.

References:

1. Розпізнавання райдужної оболонки ока [Electronic resource]. – Access mode: http://www.miui.ua/novosti/rozpiznavannya-rayduzhnoyi-obolonki-oka-yak-tse-bude-pratsyuvati-na-smartfonah/
2. Сканер отпечатков пальцев [Electronic resource]. – Access mode: https://hi-news.ru/eto-interesno/kak-eto-rabotaet-skaner-otpechatkov-palcev.html.

Dmytro Fil
Research supervisor: Mykhailo Kasianchuk
Candidate of Sciences in Physics and Mathematics, Associate Professor
Language tutor: Lilia Shtokhman
Candidate of Philological Sciences, Associate Professor
Ternopil National Economic University

AUGMENTED REALITY

Augmented reality is the blending of interactive digital elements like dazzling visual overlays, buzzy haptic feedback, or other sensory projections into our real-world environments.

The basic idea of augmented reality is to superimpose graphics, audio and other sensory enhancements over a real-world environment in real time. But these systems display graphics from only one point of view. So, the aim of our article is to present one of the newest technologies of augmented reality.

Next-generation augmented-reality systems as researchers state, will display graphics for each viewer's perspective [1]. Some of the most exciting augmented-reality work began taking place in research labs at universities around the world. In February 2009, technophiles at the TED conference were all atwitter because Pattie Maes and Pranav Mistry presented a groundbreaking augmented-reality system, which they developed as a part of MIT Media Lab's Fluid Interfaces Group [2]. They