УДК 004.49
Maksym Chornobuk[1], Nataliia Zhukova[2]
[1]student of group CST-210, National University «Zaporizhzhia Polytechnic»
[2]PhD (Philology), assistant prof. National University «Zaporizhzhia Polytechnic»

CHALLENGES AND RISKS OF THE SMART HOME

A smart home is a residence that uses connected devices to enable remote monitoring and management. These devices are connected with each other and can be accessed through one central point – a smartphone, tablet, laptop or a special hub. Door locks, televisions, thermostats, home monitors, cameras, lights, and even appliances such as the refrigerator can be controlled through one home automation system. The system is installed on a mobile or other networked device, and the user can create time schedules for certain changes to take effect.

Nowadays smart home technologies are developing with increasing speed as more and more people begin to use them. But, as any other technology, it should not come at the cost of safety and security. Here is the review of the most widespread security risks in this sphere.

Targeted Attacks are one of the most common security breaches. Smart-home devices contain a huge amount of personal information, from person's birth date to credit card details, that cybercriminals can steal via hacking if the IoT devices have software vulnerabilities. Hackers can use stolen data for misleading or blackmailing. To avoid becoming a cyber victim, do not share financial information, such as bank details, with smart devices, and always keep your devices' software updated.

Identity theft happens when hackers infiltrate the database of a smart-device company to pilfer the data of all its users. The data of thousands of users of certain smart devices can be stolen. Digital thieves can then apply for credit cards using or take out a mortgage using exposed users' information. Always care about the safety

of your online banking operations. Share minimal personal information with smart devices and regularly monitor your credit report for negative changes.

The lack of user's attention to authentication security often becomes a cause of security breach. Too often, IoT hubs that connect all the smart devices on the network are secured with just a weak password, instead of safe two factor authentication. This security lapse allows clever hackers to easily penetrate and gain access to the hub and tamper with it and other smart devices in smart home. Two factor authentication together with complex, unique passwords should always be used.

New technologies require new approaches to security maintenance. The smart home technologies will be developing and we will face new security challenges in future. Be always aware of digital security threats and follow all recommendations, so you can safely enjoy new technologies.