

УДК 004.043

Yehor Oliinyk¹, Yuliya Sobol²

¹student of group RT-810, National University «Zaporizhzhia Polytechnic»

²PhD (Philology), assistant prof. National University «Zaporizhzhia Polytechnic»

DATA CENTERS FOR PROTECTING AND STORING BIG DATA

Nowadays, people consume a lot of information from advertisements, social media, and internet resources. Billions of data bytes are hanging around us. But have you ever asked a question: “Where is all this information stored?”

There are many giant buildings in the world, which store and protect data from searching resources, medical organizations, science experiments, etc. Their name is Data Centers. We would never have the Internet in its present form if it were not for these repositories. Data center is a building or group of buildings used to house computer systems and associated components, such as telecommunications and storage systems. They process, store and distribute information, as a rule, for the corporation. It is focused on solving business problems by providing informational services.

Data centers consist of informational infrastructure (servers), telecommunication infrastructure, and engineering infrastructure. An appropriate temperature and

humidity level are maintained in such centers. Data Center security is a complex of software protecting tools, aimed at raising the level of safety for the stored information.

Protecting of information consists of two components: physical protection (systems of temperature controlling and firefighting) and cyber safety, which requires a completely different approach. Nowadays, the most common cyber threat is a DDoS attack. According to research evidences the number of DDoS attacks increased by 84 percent in 2019. In Data Center's case, hackers permeate in one of the collocation-servers and attack customers of the DC by inner network.

The reason traditional security is useless is that it can detect intrusion attempts but cannot eliminate them. Required property for protecting Data Center's system is integration with known means of virtualization, container and cloud environment, supporting of multilevel analysis of incoming, outgoing and intranet traffic to identify threats, that can pass existing protective barriers, also system control of detecting inadmissible changes in the server parameters settings, providing antivirus checking with minimal demands to computing resources, fixation system conditions to prevent installing different unknown apps.

Big Data is a designation of structured and unstructured arrays of huge amounts of information, which have great variety and enormous volume and are effectively processed by programming software tools. There are many options for protecting Big Data, such as biometrical parameters, biometrical cryptosystems, and double and triple verification if it comes to government information. However, biometrical methods cannot guarantee full protection, so modern Big Data Systems are working with combination of several identification parameters.

Security systems have come a very long way for the last thirty years, from small simple structure with physical safety and organizational measures to complicated systems which use artificial intelligence elements. However, modern technologies cannot save and protect data without specialists and daily work to identify priority threats.