CYBERSECURITY IN 2021

Vavula O.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Liakh Y. V. – Lecturer

Annotation. The problem of cyberattacks, ways to solve it from the perspective of the state and private organizations, as well as the advantages of cyberattacks for IT specialists are mentioned in the thesis.

Keywords. Cybersecurity, cyberattack, hacking, data, attack, cybercriminals, financial risk.

In our modern world, in the 21st century, when information technologies are increasingly affecting all the spheres of life, various new types and methods of theft and fraud have begun to appear. The fast-growing rise in cyberattacks around the world is costs companies dearly as they seek to better protect their computer networks from intrusions. Cyberattacks are not only becoming more frequent, but also bring great financial losses to the victims. Cybersecurity experts predict that in 2021 there will be a cyberattack incident every 11 seconds. This is nearly twice what it was in 2019, and four times the rate than five years ago in 2016. Cyberattacks are increasing in frequency, ramping up the data privacy threats they pose to government agencies and businesses alike. Governments both domestic and foreign need to step up efforts to pass legislation that bolsters technological defenses this year, warn privacy groups. Stiffer privacy laws are gradually being reviewed and signed at the U.S. market. But that process is mostly taking place at the state level [1].

Worldwide, cybercrime cost businesses, government agencies, and consumers in general more than $1 trillion in 2020. That is around one percent of the global GDP. While $945 billion was lost to cyberincidents, $145 billion was spent on cybersecurity. Those costs increased by more than 50 percent compared to 2018, when over $600 billion was spent to handle cybercrime [1].

The only sure defense is to step up efforts to pass legislation which strengthens technological protection. That may be the only way to alter the course of ongoing cyberattacks. Despite all the efforts to protect systems and data, cloud breaches are likely to increase in both velocity and scale.

The world pandemic has hastened the cyberintrusions. Over the next year, ransomware will continue to be the biggest threat and financial risk to enterprises. Most organizations should be very concerned about ransomware as the biggest cybersecurity challenge and threat. Ransomware continues to evolve into more than just a security incident. Cybercriminals now seek data breaches with organized cybercrime

groups to steal the data before they encrypt on corporate servers. Companies are not just worried about getting their data back but also who it gets shared with publicly. Cybercriminals use ransomware to target anyone, any company, and any government, hospitals and transportation industries at a time when they are under extreme pressure. One of the often-unspoken ways of safeguarding against cybersecurity assaults is education [1]. Around the world, various educational institutions have begun to introduce the study of information technology and countering cyberattacks is included in the topics studied. Various Internet resources also allow you to deepen your knowledge in this area. Many people who have faced cyberattacks and successfully coped with them without losses, post articles on Internet platforms in which they share their experience.

Owners of large companies often look for specialists in the field of cybersecurity on the Internet. The emerging field of cybersecurity is a very viable career path. Industry reports show that the number of unfilled cybersecurity jobs is expected to grow by 35 percent. The demand for cybersecurity jobs has certainly increased in the past year. A career path in the field is a great choice for anyone interested in IT and security. An increase in the number of tools utilized increases security operations and analytics complexity and requires an increase in personnel. Nearly 70 percent of security teams say it is difficult to recruit and hire additional SOC (security operations center) staff. Security analysts have the opportunity to impact more than just their specific industry. Cybersecurity reaches into the world of politics, economics, and other sectors of the world. While breaking into the field can be challenging, it is incredibly rewarding. Cybersecurity is one of the professions of the future.

Consequently, there is such a problem in the world as cyberattacks. Despite the fact that every year funds are spent on improving security, and companies employs people who understand cybersecurity and know how to prevent hacking from outside, the percentage of cyberattacks, compared to last year, has increased by 100% and continues to grow.

References*:*

1. The future of cybersecurity in 2021 and beyond [Electronic resource]. – Access mode: [https://www.technewsworld.com/story/The-Future-of-Cybersecurity-in-2021-and-Beyond-87018.html] – Date of access: 10.03.2021.