ABOUT CYBERSECURITY

Denisenko L.I., Krasnova E.V., Bukovshin V.A.
Don State Technical University

"In the XXI century, bits and bytes can be as dangerous as bullets and bombs" (William Lynn, US Deputy Secretary of Defense).

In this article we'll focus on the impact of the digital world to the world community and the importance of cyber security for the modern man.

First of all, let's ask ourselves: Can we imagine the world without the latest technology today? Can we leave the pilot of the plane without support for a moment, can we find the right way without a GPS-navigator in some desert, can we communicate with our loved ones for hundreds of thousands of kilometers without access to the World Wide Web?

It is obvious that today's society is subjected to total informatization. Global informatization manages the existence and functioning of the international community. According to unofficial data, almost half of the world's population has its own "digital profile", which means that era of open data exchange and online communication has begun. At the time, the number of "cyberattacks" increases, and they are becoming more sophisticated. Suppose that a man keeps on e-mail number and password from his credit card and other personal information. At one moment, he can't go to his email, while his account «is cleaned». In this situation, the average person can't take any measures. Therefore, the international community think about certain security of human's personal data on the Internet and the protection of the huge number of existing information systems, from some civilian communication networks, banking or exchange organizations and to military facilities. Now information technology is used for solve problems of national security, military security, economic security, etc. "Cyberspace" - the global field of the information environment, which includes a set of interdependent information technology infrastructure, including information and

telecommunication networks and computer systems for the storage, processing, modification, and data exchange. This is a strategic issue of national importance, affecting all sectors of society.

The field of computer security based on its own language and focuses on the issues of vulnerability, threats and countermeasures. Vulnerability is a parameter that characterizes the areas that are already opened to a certain type of attack. The threat is a potential form of attack on the vulnerable area. Countermeasure –is an extra step or improved design that eliminates the vulnerability. On the other hand, the threat causes to take countermeasures, and countermeasure poses new threats. In fact, countermeasure is effective if it is used properly. Computer security requires constant attention, analysis, planning and forecasting, because the protection systems that applied yesterday may be not effective tomorrow, or even today.

Computer networks also need the security, because a group of computer systems forms a whole "technical system", which needs to be protected because endanger all members of the network. Home networks may require only basic protection system, which would protect the networks from the simplest forms of information attacks. Large enterprise networks may require high-tech equipment, including high-quality hardware and decent software.

Any good defense attempts to learn as much as possible about the threats that it may face, both the tools that an adversary may use and the identity and motivations of likely attackers. In the information systems security world, it is difficult to collect information about attackers (though such intelligence information should be sought). It is, however, much easier to collect and analyze information on technical and procedural vulnerabilities, to characterize both the nature of these vulnerabilities and their frequency at different installations. Dissemination of information about these vulnerabilities enables administrators of the information systems that may be affected to take remedial action.

At present, the exact definition of the term "cybersecurity" does not exist, but most of the world understands the importance of the problem and is already involved in "cyber security strategy" adopted in the 2008.

The views on cyber security has evolved, and after the incident, September 11, 2001 changed completely. Now the area of technology, which was previously used for protection against pests, is used for a deliberate attack. As an example, the pact "On Information Security", adopted in 2008 in the US, read that counteractions by the command of the state of cybersecurity in the direction of enemies is not only possible, but is also required in this case. So now that cyberspace is considered to be a field of war, like the ocean or the airspace or the land or the space.

Let's hope for common sense of humanity and the fact that the opened opportunities will be used for peaceful and long-term for each order purposes only.

References:

1. Yuri Borodakiy (2010). Cyber security as a main factor for national and international security XXI century.
2. Computer Science and Telecommunications Board National Research Council (2011). Cybersecurity Today and Tomorrow: Pay Now or Pay Later.
3. Mikhail Bezkorovainy (2010). CYBERSECURITY - APPROACHES TO THE DEFINITION.