УДК 004.056

CYBERSECURITY

© Durasov S.V., Mishina Y.E.

e-mail: s.durasov0@gmail.com

Samara National Research University, Samara, Russian Federation

We live in the age of information technology. And nowadays the most valuable resource is information. As Rothschild said, «The one who owns the information, owns the world». But not all information should be in open access. Therefore, an important question arises how to protect information?

Protecting information depends a lot on the complexity of the password, our attention to the sites that we visit and the programs that we install on our computer. To understand how to protect it, first let`s take a look at the main ways of hacking accounts.

The first one and the most popular is – brute force which goes through all possible password combinations and finds the one you need. The success of brutforce work depends entirely on the complexity of the password. The simpler the password, the faster it will be cracked. Another similar method is dictionary attack. Attacks of this type go through the words that most people use as a password. And it makes the attack much faster [1].

Still another one is social engineering and password recovery questions. In general, the method is reduced to the fact that almost any information necessary to access confidential information can be found in the public domain. And I will give only a simple example related to passwords. As you know, on many sites for password recovery it is enough to enter the answer to the control question: which school you studied at, your mother's maiden name, your pet's name, etc. Even if you have not already posted this information in open access on social networks, do you think it’s difficult to get such information? Not at all. Either using the same social networks, being familiar with you, or specially met.

To avoid all of this use a complex password consisting of symbols, numbers and special characters. Don`t use the same password for all sites. If you have a large number of passwords, you can store them in the special password managers.

The next method, which is also very popular is phishing. The attacker makes a fake page of a popular site, which usually has a similar web address and design. As a result, users enter their login and password.Always check the website address, see that it is certified [2].

And finally, less popular, but no less dangerous – spyware represented by a wide range of programs. Not always, but most often this problem is solved by installing an antivirus [3].

References

1. Matt Curtin Brute Force. Cracking the Data Encryption Standart. -Copernicus; Softcover reprint of hardcover 1st ed. 2005 edition October 6, 2010. -304 p.

2. Christopher Atkins Phishing Attacks: Advanced Attack Techniques. -CreateSpace Independent Publishing Platform; 1 edition January 21, 2018. -160 p.

Gregory D Evans Spyware Reference & Study Guide. -LIGATT Corp.; Study Guide edition March 2005. -364 p.