Pochuyko A. S. *Cyber Attacks as a Threat to a Secure Business Environment*
The research advisor: Makutonina E. Yu., lecturer

New information technologies improve the quality of life. But, unfortunately, the introduction of modern information technologies has led to the emergence of new types of crimes, such as computer crimes and cyberterrorism - illegal interference with the work of computing systems and computer networks, a theft, an embezzlement, an extortion of computer information. Cyberterrorism is a new form of terrorism that uses computers and electronic networks, modern information technologies to achieve its goals. Moreover, nowadays the information security is one of the important components of the national security of the state. Judging by their arrangement features, their methods of concealment, cyber-attacks have a certain specificity, characterized by a high level of latency and low level of detection. Cyberterrorism has been raising a serious problem, a serious threat to the world community, this danger is compared with nuclear, bacteriological and chemical weapons.

Stages of cyber attacks. Targeted attacks are becoming increasingly sophisticated as they go through different stages:

1) espionage;
2) intrusion;
3) internal spread;
4) attack;
5) elimination of traces of activity[99].

Let's consider the causes of cyber attacks. Economically Motivated Cyber Crime. Considering crimes committed outside the Internet, money is a major motivator for many cyber criminals. The perception of low risk and very high financial rewards prompts many cyber criminals to engage in malware, phishing, identity theft and fraudulent money request attacks.

Personally Motivated Cyber Crime. Cybercriminals are often people who have been offended by someone and they want to take revenge on their offenders or other groups associated with them.

Ideologically Motivated Cyber Crime. These kinds of attacks are conducted with ethical, ideological or moral reasons, damaging or disabling computer equipment and

[99]NEC - Information Management. [Electronic resource] – Mode of access: http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html– Date of access: 17.02.2018.

networks to express grievances against individuals, corporations, organizations or even national governments.

Lack of knowledge in the field of IT. The human inability to recognize an unauthorized access leads to the illegal receiving of information, which in turn can lead to financial losses.

Malware, phishing, cyber attacks to steal IP or data, cyber attacks to steal financial information, internal attacks are main threats of cyber terrorism.

Let's move on to the impact of cyber terrorism.

Reputational damage: Trust is an essential element of customer relationship. Cyber attacks can damage your business' reputation and erode the trust your customers have for you.

This, in turn, could potentially lead to:

1) loss of customers;
2) loss of sales;
3) reduction in profits.

The effect of reputational damage can even affect relationships you may have with partners, investors and other third parties vested in your business.

Threat to life. The threat may even be to life: imagine the attacker with the ability to turn off life support systems in hospitals or take control of autonomous vehicles.

Economic damage. Cyber attacks often result in substantial financial loss arising from:

1) theft of corporate information;
2) theft of financial information (e.g. bank details or payment card details);
3) theft of money;
4) disruption to trading (e.g. inability to carry out transactions online);
5) loss of business or contract[100].

Businesses that suffered a cyber breach will also generally incur costs associated with repairing affected systems, networks and devices.

I have carried out the research based on the InfoWatch analytical center data. As a result organizations of the financial sector (about 30%) and the oil and gas industry (20%) are the most affected industries. Moreover, the data of Bank cards and accounts, personal data, information constituting a trade secret, confidential information and information relating to state secrets are the main objects of targeted attacks.

[100] Alpha IT Labs -Cyber crime is the greatest threat to every company in the world. [Electronic resource] – Mode of access: https://alphaitlabs.com/ – Date of access: 22.02.2018.

Having analyzed the data from MacAfee, I inferred that the consequences of the economic damage from cyber-attacks, along with drug trafficking and piracy are considerable. However, it should be taken into account that the estimates of losses are typically based on assumptions about their scale.

As far as countermeasures against Cyber-attacks are concerned, they involve assessing the current situation to identify assets to be protected, potential threats, and the extent of damage caused.

Preventive measures. Preventing an attack in the first place is far better than having to detect and respond to one. Such measures should include:

1) restricting user access rights and login times;
2) reviewing anti-malware and anti-virus defenses;
3) implementing anomaly detection;
4) utilizing IPS and “white-lists” to prevent connections to suspicious sites.

Human Resource Development. Companies should hire consultants with expertise in defending against sophisticated cyber-attacks who undertake theoretical evaluations to decide how to go about providing countermeasures in the future. Besides employees should be aware of the latest information technologies.

Practical security measures must be the following:

1) regularly patching firewalls;
2) updating firmware;
3) setting strong passwords;
4) changing the password your Wi-Fi router came with;
5) asking employees who use their own devices at work to install anti-virus software and to switch on firewalls.

The world wide Web is an ideal environment for terrorist activities, as it is extremely easy to access, it is simple to remain anonymous, nobody managing or controlling it properly. The cyberterrorism has been incredibly expanded by the spread of the Internet. Cyberterrorism is a socially dangerous threat to humanity, and the extent of it has not yet been fully understood and studied. That is why a cure for cyberterrorism must be a priority in the fight against any crime. Common rules for monitoring Internet information in order to prevent cybercrime must be developed by the international community.