of the trial, the reasonable term of consideration of the criminal proceedings, the term of the preventive measure, the term of bringing to criminal responsibility, etc. No matter how radical it sounds, criminal proceedings must continue even during the war. And legislative changes aimed at ensuring the capacity of criminal proceedings in such conditions should be complemented by mechanisms to prevent the manipulation of martial law in order to prolong the judicial process.

Список використаних джерел

1. Кримінальний кодекс України . 11 ч. 1 ст.

2. Проблеми протидії злочинності: підруч. Х.: Новасофт, 2010. 352 с.

3. Куц В. Зміст та рівні протидії злочинності. *Тенденції та пріоритети реформування законодавства України: матеріали всеукраїнської науково-практичної конференції* (м. Херсон, 11–12 грудня 2015 р.). Херсон: Гельветика, 2015. С. 152–156.

Салівончик А.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Гіпська Т.**

COMBAT AGAINST CYBERCRIME IN THE USA

The Internet as an invention is very useful for society, but with the advent of the Internet, new types of dangers have appeared, such as cybercrimes. Cybercrime is a general name for criminal activities that are used on the Internet, often with the intention of making money or obtaining personal information [1].

Every state cares about its citizens, and also provides information security with the help of organizations that identify cybercriminals and fight against them. One of these countries is the USA. In the USA there is a division of national significance.

The National Cyber Security Division (NCSD) is a division of the Cyber Security and Communications Directorate of the Directorate of National Security and Programs of the US Department of Homeland Security [2]. The main task of this unit is cooperation with other equally important state authorities and assessment of threats in the field of information security. The goals set for this unit are: to effectively respond to crimes in cyberspace, implementation of a risk management program to protect critical infrastructure.

The national politics y of the United States in the field of information protection is formed by the Agency of National Security (NSA), and the most important strategic issues of information security are considered by the National Security Council issued by the directives of the President of the United States, wed whose: «Politics in the field of communication systems» (1977), «United States National Security Policy in the Safety Security Systems in Automated Information and Telecommunication

Systems in Automated Information Systems» (1984) and others. USA, as well as other countries, it actively developed precisely in this direction, that is, to ensure the information security of its citizens and the country itself. If we speak in general, then there were 4 stages of US development in the direction of cybersecurity.

The main tasks of the US National Security Agency are to ensure the functioning and implementation of state policy in the field of information space. The agency is responsible for the collection and analysis of foreign intelligence, as well as for the protection of US government information systems and computer networks. It is important to note that the agency is engaged in cryptological intelligence, and it is also part of the US Department of Defense.

The National Security Agency of the United States is an integral part of the country's security system along with the Central Intelligence Agency and other agencies, but unlike the Central Intelligence Agency, it does not engage in the use of agents in other countries. According to the federal law, the activity of an agent [3].

In addition to the US National Security Agency, its issues in the field of cybercrime prevention are also regulated by certain regulatory legal acts. Their general meaning is that they:

– determine the objects of legal protection in the information sphere;

– determine the procedure for realizing ownership of information objects, the rights and obligations of owners;

– determine the legal regime of functioning of information technologies;

– determine the categories of access of individual subjects to certain types of information;

– establish categories of secrecy;

– define the concept of «confidential information» and the limits of its legal application [4].

Therefore, organizations and agencies of the USA have achieved large-scale development in the fight against cybercrime and continue to further improve the system of information security.

Список використаних джерел

1. Кіберзлочинність: як ідентифікувати та як діяти. URL: http://safe-city.com.ua/kiberzlochynnist-i-litni-lyudy/.

2. Національне управління кібербезпеки США. URL: https://uk.m.wiki.org/wiki/Національне_управління_кібербезпеки_США

3. Центральне розвідувальне управління. URL: https://uk.m.wikipedia.org/wiki/Центральне_розвідувальне_управління.

4. Система захисту інформації в США. URL: https://narodna-osvita.com.ua/2448-tema-10-sistema-zahistu-nformacyi-v-ssha.html.