Ворошко Г., Козін О.,
студенти 2 курсу групи ПБі-18-1 ННІ права
Університет державної фіскальної служби України
Науковий керівник: **Кузько І.В.,** старший викладач кафедри сучасних європейських мов УДФСУ

CYBERCRIME PREVENTION

Cybercrime is a crime that consist a computer and a network. Today these crimes have become very common. Cybercrime are committed with use modern telecommunication network such as Internet (Bluetooth, SMS, MMS) for the purpose of to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly. Cybercrime may be threaten the security of a person and their financial situation.

The main aim of cyber criminal is computer system that manages various processes, and the information that circulates therein. Unlike ordinary criminal, which acts in the real world, cyber-criminal doesn't use traditional weapons such as a knife or a firearm. His arsenal includes information weapons, all of the tools that are used to penetrate the network, cracking and software modification, unauthorized information or to block the operation of computer systems. To cybercriminal's weapons we can add computer viruses, backdoors, various types of attacks that make possible a more effective and unauthor - used access to a computersystem. In the arsenal of moden computer criminals there is not only the traditional media, but also the most modern weapons and equipment information. All issues, which related with solving computercrime, have crossed national border sand havegained international significance for a longtime [1].

According to the Convention, each State Party must provide the necessary legal conditions for the provision of the following rights responsibilities of the competent authorities to combat cybercrime: seizure of a computer system, part or carriers; manufacturing and confiscation of copies of computer data; to ensure the integrity and security of stored computer data relating to the case; destruction or suppression computer data in a computer system. The Convention also requires to create the necessary legal conditions oblige ISPS to collect and fixation or intercept the information you need with the help of available technology, as well as contribute to this law enforcement. It is recommended to oblige providers maintain complete confidentiality about the facts of this cooperation.

In many countries of the world in order to suppress the fact the information crimes in recent years, computer security experts began a collaboration with psychologists, who make up the profile of the so-called hackers, that is criminal in the sphere of computer information and technology, which allows to identify the level ofskills and technical training. But it should be noted that while computer experts can tell a lot about hackers and its methods of work, but they will never be able to understand the psychology of his criminal thinking. These issues are dealt clinical psychologists, forensic experts and other specialists together with the police This practice is widely used in the United States, Europe and other countries where cybercrime is widely developed. But due to the fact that under current conditions a significant portion of the fight against cybercrime, as well as with other international crimes, belongs to the domestic jurisdiction of each state, it is necessary to develop parallel and national legislation aimed at combating computer crime, coordinating it with the international standards Law and relying on existing positive experience [2].

So combating cybercrime is very important now, because cybercrime is spreading all over the world. Each state should ensure the implementation of state policy in the field of combating cybercrime, organize and carry out, in accordance with the law, operational search activities.

Список використаних джерел

1. Journal “Law and justice statistics”.
2. Aratuly “International cooperation in the fight against cybercrime”.

Гавриленко О.,
курсант Національної академії внутрішніх справ
Консультант з мови: **Гончаренко Н.І.**

CRIMINAL INVESTIGATION TASK FORCE AND NATIONAL CYBER INVESTIGATIVE JOINT TEASK FORCE

The Criminal Investigation Task Force (CITF) - is an organization created in early 2002 by the United States Department of Defense to conduct investigations of detainees captured in the War on Terrorism. It was envisioned that certain captured individuals would be tried by a military tribunal for war crimes and/or acts of terrorism. CITF was initially activated in February 2002 under a mandate from the Secretary of Defense addressed to the Secretary of the Army. The Secretary of the Army formally tasked the US Army Criminal Investigation Command (CID), and CID activated the Criminal Investigation Task Force solely for the purpose of conducting