PECULIARITIES OF COMBATING CRIMINAL OFFENSES UNDER MARTIAL LAW

Due to the start of the war on February 24, 2022, martial law was introduced in Ukraine. In connection with it a decision was made to amend the Criminal Code of Ukraine, which increased criminal liability for a number of crimes under martial law. Thus, according to Clause 11 of Part 1 of Article 67 of the Criminal Code of Ukraine, the commission of a crime under martial law is an aggravating circumstance for punishment [1].

For a more convenient understanding, we note that this is the use of a more unfavorable time period for society, difficult circumstances and conditions by the guilty person, which may indicate an increased degree of social danger of crimes committed under martial law.

Undefined and unsettled issues in the spectrum of criminal proceedings are a problem of conducting criminal proceedings in martial law. Since the tasks of criminal proceedings remain unchanged, but the mechanisms for achieving the goals cease to work in the conditions of martial law. According to the Law of Ukraine «On the Legal Regime of Martial Law», courts, bodies and institutions of the justice system are authorized to work only within the limits of the powers defined by the Constitution and Laws of Ukraine.

The first means of crime prevention is the prevention of criminal offenses. It consists in neutralizing the criminogenic prerequisites of a possible offense, or activities aimed at eliminating and neutralizing the reasons for its possible commission, as well as the conditions that contribute to it. When prevention turns out to be insufficiently effective, there is a need to apply the second means of prevention – the prevention of a criminal
offense. Warning is a set of measures directly aimed at the consciousness of specific individuals or individual groups of them, who have criminal intentions and plan to commit a crime. At the level of individual crime prevention, a warning manifests itself as informing a potential criminal about the irrationality of his planned criminal offense. The main feature of this form of prevention is the presence of efforts applied to specific individuals who intend to commit a crime. From the point of view of criminal law, this means that prevention of a crime is the activity of prevention subjects at the stage of detecting the intent to commit it.

If a warning does not stop a potential offender and he starts preparing to commit a criminal offense, the third, last mean of crime prevention is applied – stopping the actually started creation of conditions for committing a criminal offense, i.e. stopping preparations for committing it. The suspension remains in the sphere of preventive activity, provided that the act committed in the process of preparation is not criminally punishable. If preparation for a crime is subject to criminal liability, the termination of such preparation should be considered not as a means of prevention, but as a legal response to its commission. Stopping a crime even at the stage of an attempt to commit it should be considered legal response, not prevention, because an attempt is recognized as a criminal act [2].

In the process of criminal law response to the commission of offenses, another relatively independent direction of countering crime is implemented – prevention of new crimes. As with the two previous levels of countermeasures, criminal-justice prevention is carried out in stages, starting with the prevention of criminal offenses, i.e. with the neutralization of the reasons for committing the offense and the conditions that contribute to it. If the specified measures are ineffective, a warning to commit a criminal offense is applied, mainly due to the subject’s assurance of the irrationality of such an act. In the case of ineffectiveness and prevention, the authorized subject can terminate the criminal offense that has begun by the means provided to him by law [3].

Therefore, the criminal justice authorities first respond accordingly to the fact of the commission of a crime, and during the criminal proceedings they prevent new crimes according to the above algorithm, and this process continues constantly. The two-component complex of criminal justice counteraction to crime is a kind of permanent tool at the disposal of criminal justice bodies, which must be professionally applied and improved.

Therefore, the essence of combating crime is the implementation of social management activities, including the implementation of public and private initiatives and criminal justice efforts aimed at keeping crime within socially acceptable limits, the content of which is the prevention of such offenses and the legal response to them as interconnected continuous processes. In conclusion, it should be added that martial law is a legal regime that is indefinite in time and unpredictable in terms of circumstances. On the other hand, criminal proceedings always have specific or reasonable time points – the term of the preparatory court session, the term of the appointment
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 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, whose: «Politics in the field of communication systems» (1977), «United States National Security Policy in the Safety Security Systems in Automated Information and Telecommunication