Vasyl M. Stratonov. "Computer crimes": some features and characteristics. Unfortunately, along with positive achievements, informatization also has negative manifestations, namely, the possibility of using computer technology to commit crimes. The world has long been talking about "cybercrime" about "computer crime," and chapter 16 of the Criminal Code of Ukraine deals with crimes in the use of computers, computer systems and networks, as well as telecommunications. Therefore, we can state that a unified approach to the definition of a concept does not exist. However, the introduction of certain norms into the law does not solve the problems. Problems arise with the direct implementation of these standards in every-day life. Since “computer crimes” are transnational in nature, we must join forces to combat such crimes. In developed countries, this type of crime leads to huge losses, significant funds that are spent on the development and implementation of software, technical and other means of protection against unauthorized access to information, its distortion or destruction. With this in mind, it is fundamentally important to study methods of committing crimes using computers, computer systems and telecommunication networks. Therefore, we characterize some of the most common ways of committing computer crimes.

Such crimes are characterized by the following features: the complexity of their detection and investigation, the difficulty of proving in court, the high damage even from one crime. Therefore, based on the analysis of both theory and the results of practice, we primarily focus on individual methods of com-mitting “computer crimes”. We reveal in the article the content, forms and methods of committing computer crimes in the realities of today.

We focus on the main methods of unauthorized receipt of information, namely: the use of a de-vice that listens (bookmarks); deleted photo; interception of electronic radiation; hoax (disguise for sys-tem requests); interception of acoustic radiation and restoration of printer text; theft of media and indus-trial waste (garbage collection); reading data from arrays of other users; copying storage media with overcoming protection measures; masking a registered user; use of software traps; illegal connection to equipment and communication lines; failure of defense mechanisms.

We characterize the most common both methods and methods of unauthorized receipt of information from computer and information networks. Knowing the ways of committing crimes will help to further prevent the commission of crimes, take preventive measures.

Keywords: *commission methods, computer crimes, automated systems, technical protection, forensics.*