COMPUTER CRIMES

Reshetnik A., *student U-75*, Piddubniy V., *student ES-71*,
Pochatko T.V., *EL adviser*

Computer crime has increased considerably since the mid-1960s, but its true extent remains unknown. Quite apart from the difficulty of defining computer criminality, and apart from the absence of clear legislation in many jurisdictions, computer criminality shares with other forms of economic crime the difficulty of detecting it. Most such crimes some investigators claim as many as 99 percent – are not reported because publicity about a company's problems with their computers may undermine the public's trust and confidence in that institution.

The number of reported computer crimes may seem to be insignificant, but many of those that have been successful have profits. Some investigators have estimated the total annual losses through computer fraud to be as high as $ 5 billion.

Let us look at the various types of computer crimes to see what they have in common and how they differ. Investigators of computer crime generally focus on activities that entail access to the computer's hardware and software. Most such acts have in common a loss to the rightful owner of data, and often the perpetrator gains financially. But this need not be the case. Some computer crimes may even pose a threat to the national security.

- Computer fraud involves the falsification of stored data or deception in legitimate transactions by manipulation of data or programming, including the unlawful acquisition of data or programs for purposes of financial gain of the perpetrator or of a third party.
- Computer espionage consists of activities by which unauthorized computer access steals information for purposes of exploitation from databases belonging to government or private parties.
- Computer sabotage consists of the tampering with, destruction of, or scrambling of data or software by means of gaining access to data banks.
- Computer hacking is the act of gaining unlawful access to data banks for malicious, though not necessarily destructive purposes, and for neither financial gain nor purposes of espionage.
- Theft of computer time, software, and hardware includes not only the unauthorized use of computer time and software services but also the unauthorized copying of software programs, and the outright theft of computer equipment.

So far, most known computer crimes seem involves manipulations for purposes of fraud or industrial espionage. But the number of computer nuisance crimes, including sabotage and hacking, has been increasing, and thefts of computer time and software are predicted rise rapidly.