In recent years, cybercrime has become an increasingly serious problem, and the age of those who commit such crimes is rapidly declining. Young people are actively involved in hacker activities using their technical skills for illegal operations. At the same time, technologies, such as artificial intelligence (AI), open up new opportunities for attackers. Irina Pantina, teacher of the Department “Information Protection” MSTU named after N.E. Bauman, Head of the Department of Methodology and Technology of the Department of Information Security, ANO “Digital Audit” told why cybercrime is the youngest and how II becomes an instrument of attacks.

According to the Ministry of Internal Affairs of Russia, the number of crimes in the field of information and telecommunication technologies among minors for the period from 2020 and to 2024 increased 74 times. One example was the operation in St. Petersburg, where in March 2024 Detained 16-year-old teenager. He was suspected of unlawful access to computer information and cooperation with fraudulent call centers. The investigation believes that the young man served equipment for replacing telephone numbers and received payment in cryptocurrency. He worked from rented apartments, where he installed GSM-goals, used thousands of SIM cards and laptop. In order not to get caught, he regularly changed housing and SIM cards.

Irina Pantina in the framework of the Forum “Territory of the Future. Moscow 2030 ”said that the average age of hackers today is 25–35 years, but younger are often involved in criminal activity. It all starts with interest and experiments – from attempts to hack for the sake of excitement to turning into a source of income.

> Many hackers actually lead the familiar “office” lifestyle: they go to work and receive salaries, only this salary is for criminal activity.

Irina Pantina
Head of the Department of Methodology and Technology of the Department of Information Security, ANO “Digital Audit”

A separate threat is the use of artificial intelligence. Technologies allow you to create fake audio and videos that are difficult to distinguish from the present. For attacks, it is enough for a person to post several videos or records with his voice.

> If a person posts a video with his voice, the neural network can learn and use it

for attacks, for example, call relatives already with “your voice”. The more digital traces we leave on the Internet, the higher the probability of becoming a target.

Irina Pantina
Head of the Department of Methodology and Technology of the Department of Information Security, ANO “Digital Audit”

Pantina recalled that the use of technology is not limited to small fraudulent actions. The history of cybercrime already knows examples of attacks that have changed political and economic processes. Among them are the Stuxnet virus, which stopped the work of the

Iranian nuclear program, a leak of Hillary Clinton’s correspondence during a presidential campaign in the United States, attacks on Aeroflot, as well as cases of industrial espionage against large international companies.

According to the expert, the main measure of protection remains attentiveness and caution on the Internet.

> It is important to filter the information, be careful about publishing personal data and be attentive to sources. Vigilance is the first step to digital security.

Irina Pantina
Head of the Department of Methodology and Technology of the Department of Information Security, ANO “Digital Audit”

Thus, cybercrime not only grows, but also rapidly becomes younger. In conditions when artificial intelligence is used to create fakes and new attack circuits, protecting personal data becomes the task of not only specialists, but also each user.