UDK 004.056.5:811.111

FRIENDLY HACKING METHOD

Kabak V. S., student
Scientific supervisor – Turchenuk M. E., lecturer
Belarusian National Technical University
Minsk, Republic of Belarus

I have learned one thing: in any game there is always an opponent and there is always a victim. The whole trick is to realize in time that you have become the second, and become the first.

The concepts of Red Team and Blue Team came from the traditional military craft, and the essence of these terms has not changed at all. Blue Team in the context of cybersecurity means a team of experts whose task is to ensure the infrastructure protection.

The tasks of the Blue Team are divided into the following areas:

– prevent – build a protection system against already known attacks;

– detect – identify new (including previously unknown) attacks and promptly prioritize and handle incidents;

– respond – develop response measures and policies in order to identify incidents;

– predict – predict the appearance of new attacks taking into account the changing threat landscape. The last point from a technical point of view brings a real challenge to the work of a security analyst. This block includes measures to assess the level of security, but they also allow you to evaluate the effectiveness of processes at other stages. Thus, the task of the Red Team is not to "smash" the corporate infrastructure and prove to everyone that everything is bad; on the contrary, it is to use security analysis as a constructive measure to evaluate existing processes and help the Blue Team improve them. In many organizations where the #IB processes are not yet mature enough, the tasks of security assessment are solved by Blue Team specialists. Occasionally there are large companies that also add the Purple Team. Purple experts help other teams to be friends, allowing the blue team to develop a strategy and technical measures to protect the infrastructure based on the vulnerabilities and shortcomings discovered by the red team.