УДК 004.8
Kirill Kladko[1], Olha Kalantaieva[2]
[1]student of group RT-818 ZNTU
[2]teacher ZNTU

ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Now there is a unique situation in the field of technology that provides the Internet, such that it has become very easy to automate the search for software vulnerabilities and their exploitation. What is a software vulnerability? This is a bug in a program that allows someone who knows about it to do something useful for him.

This kind of error has become possible to search automatically much more efficiently than it was before. This is due to the fact that web technology has become the main platform for applications. Many applications have moved to the web - social networks, mobile offices, which are directly accessible through the web. And now, less often than before, people work with documents only locally, and very often work collectively through cloud services and so on. And it turns out such a picture, which previously simply did not exist. Both the server side and the client side, that is, the client devices themselves, are available 100% of the time, seven days a week via the Internet via very good communication channels.

From this emerges such a feature: all copies of popular programs that are vulnerable are available at arm's length. If I searched some popular program on my computer, I found an error in it that allows me to do something in another instance of the same program, I can scan the Internet in a few minutes, find all the copies that are online now, and Run this error. That is, the infrastructure itself is now conducive to automation.

What is artificial intelligence? These are, as a rule, sets of algorithms that automate typical tasks that a living being does — a human being in this case. That is, if you look at the theory of artificial intelligence, they emit such intelligent agents. Agents are someone who works in the environment. In our case, when we are talking about cybersecurity, the environment is the programs that are accessible and connected by the network. We see their interfaces - and those interfaces that people see, and those interfaces that are only for machine-readable interaction. And in this environment, which can be perceived by an intelligent agent, he can very quickly and efficiently look for subtle places in how the application that he explores is implemented.

Automatic robots that can be written, as a rule, do much better with combinatorial and combinatorial tasks than humans. This is where you can invent new algorithms, optimize brute force, determine what needs to be dug in this direction, give exactly this type data, and not some other, quickly generate a lot of examples and watch the response on each of them.

As a result, AI is used not only by hackers to find vulnerabilities and their further exploitation, but also to find these holes, but already to fix them. And now, using AI, you can quickly get rid of many system vulnerabilities before take advantage of hackers.