Model for vulnerabilities detection in unmanned vehicle interfaces based on artificial immune systems

A. V. Skatkov¹, D. V. Moiseev¹ and A. A. Bryukhovetsky¹

¹ SEVASTOPOL STATE UNIVERSITY, 33 Universitetskaya str., Sevastopol, Russia, 299053
Abstract.

• The development of artificial intelligence (AI) and unmanned vehicles (UMV) built on the basis of AI use requires paying great attention to information security (IS) issues. For this purpose, we propose the use of the artificial immune system (AIS) apparatus as a heuristic method for detecting incidents of intrusion into the UMV security infrastructure, where the IS plays a special role in the channels of information exchange. In this paper, we study mathematical models of immune response enhancement of AIS, which are systems of ordinary differential equations. For the first time, it was proposed to consider the degree of damage to the UMV resource (s), and, as a result, their ability to effectively perform protective functions; to consider UMV virus attacks as a multiplicative function; to accumulate an antivirus database ahead of time to improve the effectiveness of anti-virus measures.
The mechanism of the immune response of the immune system counteracting the antigen.
Results of modeling the immune response of the AIS
Conclusion

Used so far the expression describing idealized behavior of the infected organism (damaged resource), which is not taken into account the impossibility at a certain level of organ damaging (resource) to perform an immune response, modified by authors using the introduction of non-increasing non-negative functions, taking into consideration the malfunction of the immune system due to considerable destruction of the organ (resource).

For the first time in order to correctly describe the mechanisms of AIS for UMV, we propose to consider the destruction of BTS resources by viruses as a multiplicative function.

The anti-virus database (the relative volume of the anti-virus database) is formed with a delay in accordance with classical mathematical models, since the AIS analogy is based on classical models of immune systems. In our opinion, it is necessary to accumulate an anti-virus database ahead of time.

Creating an anti-virus database ahead $C^*(t)$ brings a positive effect in the speed of reducing the volume of accumulated viruses $V^*(t)$ and improving the efficiency of anti-virus algorithms $F^*(t)$.

The analysis of the obtained results allows us to conclude that the modification of classical mathematical models in accordance with the specifics of the AIS has significantly increased their adequacy and allows using the methods of the AIS to detect vulnerabilities of the UMV interfaces.