

УДК 621

Maksym Vereshchaka¹, Olena Syvachuk²

1 PhD student, RET Dpt., NU “Zaporizhzhia Polytechnic”

2 senior teacher NU “Zaporizhzhia Polytechnic”

MODELING OF INFORMATION SECURITY PROCESSES IN TECHNICAL SYSTEMS

Antiviruses are one of the most effective means of protection against information security threats. If an operating system is not protected by an antivirus program, it can become infected with malicious software objects, which can ultimately lead to a threat to information security.

When analyzing suspicious files, VirusTotal provides diagnostics provided by the world's leading commercial antivirus products. When it comes to suspicious web servers, VirusTotal uses a database that is responsible for detecting virtual addresses using malicious methods.

VirusTotal has an Application Programming Interface (API) that allows programmers to query the platform automatically without using a graphical web interface.[1] This document has two APIs that VirusTotal hopes for. The first requests for uploading files to the platform server. The second API is to make commercial anti-virus diagnostics available for files uploaded to the platform by the first API.

As for the first possibility of VirusTotal, the antivirus detects the maliciousness of the suspicious file. In the proposed experimental environment, all sent executable files are malware. Therefore, in the proposed study, the antivirus is triggered when it detects the maliciousness of the file under investigation, which is being executed. The detection of malicious programs indicates that the antivirus provides reliable protection against cyber-intrusions. The larger the blacklist database is, the better the antivirus protection is.

In the second possibility, the antivirus confirms the benign quality of the file under investigation. Therefore, in the proposed study, when the anti-

virus confirms that the file is benign, it is a case of false negative because all samples are malicious. That is, the examined file is malicious software. However, the antivirus incorrectly indicates benignity.

In the third possibility, the antivirus does not report a suspicious file being executed. An oversight indicates that the examined file has never been evaluated by an antivirus and does not have sufficient reliability to be evaluated in real time. The lack of antivirus diagnostics indicates its limitations in large-scale services.

Not all modern antiviruses are able to resist even currently known information security threats nor are they able to resist them at a sufficient level. In order to develop the competitiveness of antiviruses with a lower level of protection, it is necessary to develop a greater number of protective components, as well as to regularly monitor and respond to the emergence of new modern information security threats, so the protection of the information system must be comprehensive and include software and hardware firewalls, antiviruses, and proper operating system settings.

REFERENCES

1. Sidney M.L. de Lime, Heverton K. de L. Silva et al. (2020) Artificial intelligence-based antivirus in order to detect malware preventively. *Progress in Artificial Intelligence (electronic journal)* // [Электроний пецыпс]. no. 10(2), pp. 1-22. Режим доступа: Retrieved from: https://www.researchgate.net/publication/345943461_Artificial_intelligence-based_antivirus_in_order_to_detect_malware_preventively// [Электроний пецыпс]. (accessed 19 March 2023)