

УДК 004.94

Kvitkovskyi Ivan¹, Altukhova Tatiana²

¹ student of the group IPZm-23 of Donetsk National Technical University

² associate professor of Donetsk National Technical University

MODELLING THE PROCESS OF THREATS ATTACK ON INFORMATION SYSTEM USING PETRI NETS

Currently, information plays a rather important role in the entire world community, as it provides direct transmission of knowledge, any events, description of feelings and emotions and, in general, is considered a rather powerful weapon for manipulating consciousness and events and their possible consequences, general public opinion and the formation and influence on the assessment of events that have taken place [1]. The development of information and telecommunication technologies and the latest methods of information processing has now led to the rapid development of all modern possibilities of scientific and technological progress, global information and technological development in society. However, the rapid development of informatisation has led to the rapid emergence of problems directly with information security both in Ukraine and around the world, which, in turn, are divided into problems of information protection itself and protection against information threats, therefore, given their danger, the issue of their prevention and neutralisation requires rather strict decisions and appropriate actions, which determined the relevance of studying the impact of information threats using modern intellectual modelling methods [2].

Protection in information systems involves a certain specificity, which is associated with the fact that information is quite easily and quickly copied and transmitted through communication channels, thereby ensuring security breaches both from external and internal offenders. However, given that IT technologies are developing more and more every year, it is the security breachers who are directing their actions to find more effective tools and develop malware that will not be able to be countered by modern security systems. The stages of cyber threat research in this area involve the performance of certain operations, which are shown in Fig. 1 [2]. Therefore, the use of Petri nets to create a simulation model for studying threat attacks will make it possible to identify possible risks to information systems.

In the process of developing the model, it is necessary to understand that when a user's information system is affected by a virus element, the sets of its

vulnerabilities and existing damages that occur in the systems may change. Therefore, taking this into account, the detailing of the event of ‘damage’ to the operating system occurs by applying the definitions of partial or complete damage, as well as directly by the process of its recovery (Fig. 2). When this process is completed, two states of the system will be determined, namely the successful implementation of a cyberattack by a security breach and the information system will be considered compromised, and the normal, operable state of the user's system. The Petri net used for the process of modelling a threat attack on an information system can be represented as a tuple [3, 4]:

$$N = \langle P, T, I, Q, M, Z, S \rangle, \tag{1}$$

where $P = \{p_0, p_1, p_2, \dots, p_n\}$ – finite set of events; $T = \{t_1, t_2, t_3, \dots, t_v\}$ – finite set of transitions; $I(t) = p$ – an input function that determines the multiplicity of input transition paths; $Q(t) = p$ – output function that determines the multiplicity of output transition paths; $M = \{m_1, m_2, m_3, \dots, m_w\}$ – labelling, at that, $m_i = m(p_i)$; $Z = \{z_1, z_2, z_3, \dots, z_w\}$ – parameters of the time delay of markers in the network positions; $S = \{s_1, s_2, s_3, \dots, s_w\}$ – parameters for the timing of markers in network positions [4].

The study of the attack of information threats using the obtained UML state model was carried out at three stages: first, simulation of the intruder's actions using a virus (Fig. 3, a), second, simulation of user actions during and after a cyberattack (Fig. 3, б), and third, direct infection of the system with a virus application (Fig. 3, в).

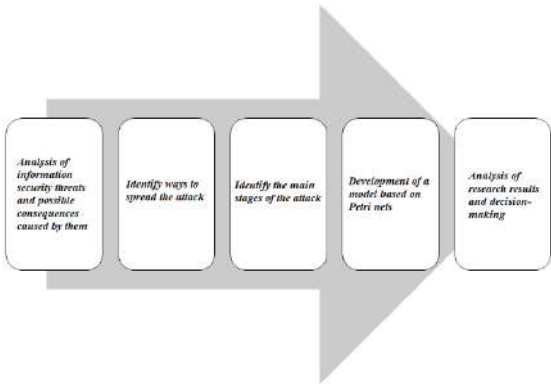


Figure 1 - The main stages of modelling the process of attacking an information system

Based on the results of the study at all three stages, a graphical representation of the time course of the information system was formed (Fig. 4).

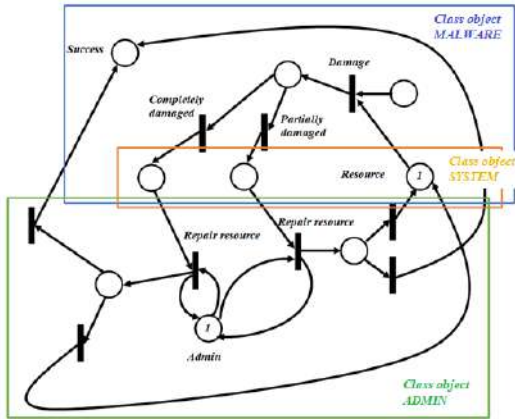
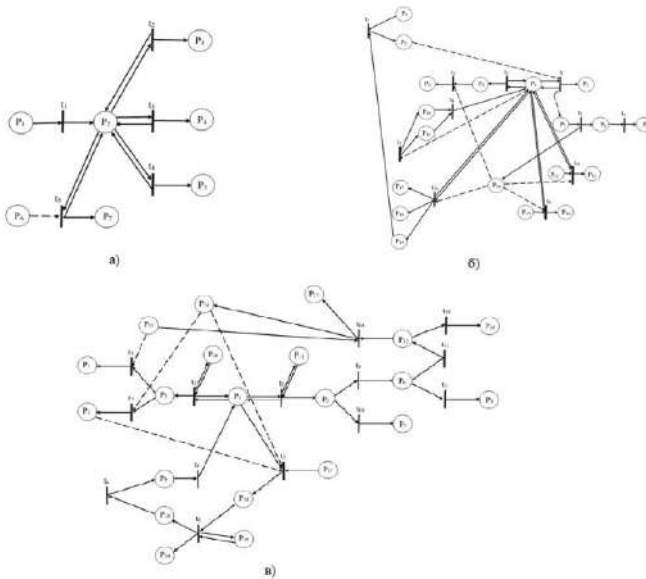
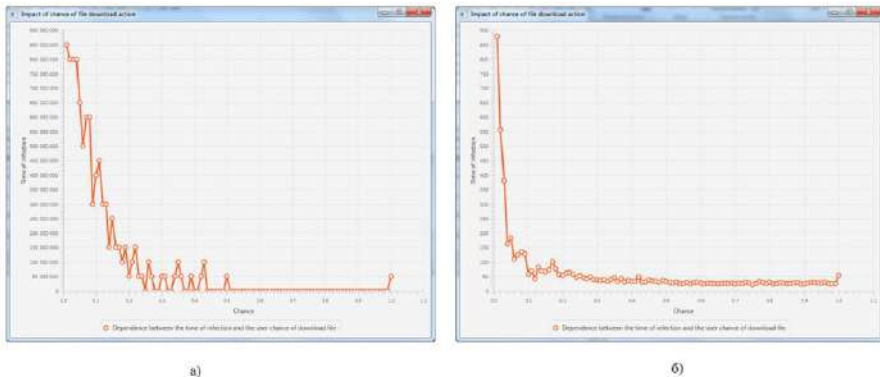


Figure 2 - UML state model for studying a security breach attack using a dangerous virus software application on an information system



a - if the security breacher performs actions; б - if the IS user acts during and after the cyberattack with a virus code; в - if the virus code is infected and the breacher is masked

Figure 3 - Formalised models based on Petri nets



a - the usual time range of the probability of downloading a malicious file; б - the time range of 100 seconds of the probability of downloading a malicious file
Figure 4 - Results of the study of the impact of a malicious virus application on the state of a computer during its infection

Based on the results obtained, it can be concluded that if the possibility of opening a dangerous virus application is increased, the time of damage to the information system by a malicious virus application will be the shortest, i.e. from 0 to 20%, the time of vulnerability is longer, with an increase from 25% it decreases. Thus, if up to 50% of the possibility of downloading malicious software to a computer is given a chance to leave it unharmed, but after exceeding this limit, a security breacher, having carried out a cyberattack using a virus, will achieve its goal of violating the confidentiality, integrity and availability of information.

REFERENCES

1. Рудий Т. В., Томаневич Л. М., Руда О. І. Засади захисту інформації в інформаційних системах підприємств. Актуальні проблеми економіки, №2, 2014. - С. 551–557.
2. Бакін Д.С. Проблеми захисту інформації в комп'ютерних мережах. Матеріали Всеукраїнської науково-практичної конференції «Актуальні задачі та досягнення у галузі кібербезпеки», 23-25 листопада, 2016 р. – С. 79-80
3. Мережі Петрі: Методичні вказівки до лабораторної роботи № 9 / Укл.: В.А. Висоцька, Т.В. Шестакевич. – Львів: Видавництво Національного університету "Львівська політехніка", 2016. – 12 с.
4. Алтухова Т.В. Комп'ютерне моделювання систем діагностики технічного стану електродвигунів гірничих машин: автореф. дис. канд. техн. наук. Покровськ, 2021. – 28 с.
5. Zaitsev D.A., Shmeleva T.R. Simulating Telecommunication Systems with CPN Tools: Students' book / Odessa: ONAT, 2006. – 60 p.