Information security system model in the automated system
developed in the simulation software environment CPN Tools

O I Bokova, S V Kanavin, V A Meshcheryakov and N S Khokhlov

Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation, 53,
Patriots Avenue, Voronezh, 394065, Russia

E-mail: o.i.bokova@gmail.com, sergej-kanavin@rambler.ru, netshuttle@mail.ru,
nikolayhohlov@rambler.ru

Abstract. This article through simulation provides the functioning mathematical model of
information security system (ISS) from unauthorized access (UAA) in automated systems
(AS). The model is developed in CPN Tools software environment for its analysis, getting
probabilistic-temporal characteristics and its further comparison with the analytical model. The
systematic analysis of functional components in ISS from UAA highlighted its key subsystems.
Integrated CPN Tools breaks the model into subsystems by preserving ISS functioning logics
from UAA, and observes the taking processes. This model performs the computation
experiment, namely, researches ISS real consumer properties from UAA in AS, which in
following researches provides the analysis software complex development and qualitative
assessment of the similar systems functioning. Simulation results of ISS functioning process
from UAA in AS can be various characteristics of each state, describing the system work both
generally and for its subsystems. The programming Metalanguage, used in CPN Tools adjusts
the simulation model and controls the marker random transition from the initial state
to final through intermediate, determines transition properties, enters different marker types, sets time
delays, etc. The article substantiates the required transitions by ISS simulation model from
UAA in AS to get reliable characteristics as the further research direction.

1. Introduction

The modern stage of the human life is characterized by the deep information, which is related to
development, exploitation of automated systems with various purposes. Due to that the attackers are
constantly improving the ways to get confidential information. In order to prevent the attempts of the
unauthorized access in the automated systems the information security systems from the unauthorized
access are introduced [1, 2]. Often regular users of such systems ignore their authorities and violate the
rules of working with secured systems. User errors are the most common, therefore at work we admit
that a mistake was made and the malware penetrated in the automated system [3]. Let us assume that
the intruder is internal with high potential. We are to consider this case for the removable information
carrier CD/DVD/HD/Flesh.

The malware can be implemented as a separate software product (SP) with the auto-start function
when connected to a personal computer (PC) in case, when the user disables the antivirus software
(SW), as the automated systems consume a large amount of resources and therefore it becomes
inconvenient to work and often it is impossible due to the heavy workload [3].
These aspects should be accounted for development and exploitation of the information security systems from the unauthorized access to determine its probabilistic-temporal characteristics as the time to perform security functions to be used further for assessing the efficiency of its functioning [4], to set interconnections of its subsystems and components, and also to build its logical structure in general. This task can be solved by constructing the imitation model of information security system from the unauthorized access, to predetermine further the above listed characteristics.

As the program environment to build the simulation model in this article we use the program developed at Aarhus University (Denmark) – CPN Tools [4–7]. A distinctive feature of CPN Tools is the availability of extensive tools, allowing to analyze the various aspects for functioning of the models based on Petri networks [9,10] (security and limited positions, the level of transition activity, availability of dead-end markings, etc.). CPN Tools are used in a variety of real projects in the sphere of telecommunication, for modeling networks and network devices, verification of communication protocols, etc. In this environment to build the models the hierarchical, temporary, painted Petri nets are used, which are the universal algorithm system. Simulation modeling in CPN Tools is the discrete-event, which presupposes an instant change in Petri net state at certain time moments.

2. Modeling
Modeling of information security systems from the unauthorized access is a complex process. The initial stage of the model development is simulation of its subsystems and their components, which are completely identical to the really functioning information security systems from the unauthorized access for getting its properties and characteristics [1, 2, 11–15]. The performed analysis proved that the model may consist of the following subsystems:

- subsystem "PC-enabling and user identification";
- subsystem "Initialization of the user rights to work in the system and access to the file catalogue";
- subsystem "User's work with files and programs";
- subsystem "User's work with applied software";
- subsystem "Destructive impact on the information security systems from the unauthorized access".

We are to introduce the following designations for peaks and transitions. Peaks in our model are used of two types with indices r1 etc and they are the functions performed by the information security systems from the unauthorized access and the peaks with indices r01 etc are complementary needed to enter probabilities. And accordingly the transitions with indices t1 etc are basic and t01 etc are complementary.

The first model displays the user's input into the information security system from the unauthorized access through its authorization (figure 1). This model provides the visual representation of what is going in the system at user's input. From figure 1 it is clear that if the password is incorrect (after the third entering) the PC is blocked, which allows providing PC security from the brute force. Transition t01 provides the marker transfer into the subsystem "Initialization of the user's rights to work in the system and access to the file catalogue in the system". Table 1 gives various states of the viewed subsystem.

The second model displays the subsystem "Initialization of the user's rights to work in the system and access to the file catalogue" (figure 2). In position r241 there is the input from the subsystem "Destructive impact on the information security systems from the unauthorized access". After the user's transfer to work with the carrier the malware program is launched automatically and in the simulation model there is a new "marker", which is the destructive software impact on the information security system from the unauthorized access directed to getting an access to information. Table 2 gives the state of the viewed subsystem.
Table 1. PC enabling and user's identification.

| Functions performed by the information security systems from the unauthorized access |
|-------------------------------------------------------------------------------------|
| 0 Launch of the information security system from the unauthorized access            |
| (Discontinuation of the information security system from the unauthorized access)  |
| 1.1 Identification provision                                                        |
| 1.2 Identification shutdown                                                        |
| 1.3 Access to the password entering                                                |
| 1.4 Password entering                                                              |
| 1.5 Password re-entering                                                          |
| 1.6 Blocked entering into the system at three-time incorrect password entering     |
| 1.7 System subject authentication                                                  |
| 1.8 Login                                                                          |

Figure 1. PC enabling and user’s identification.

Table 2. Initialization of the user’s rights to work in the system and access to the file catalogue.

| Functions performed by the information security system from the unauthorized access |
|-------------------------------------------------------------------------------------|
| 1.8 Login                                                                          |
| 2.1 Comparison of the external carrier and user identification information         |
| 2.2 Device control (if the device is not belonged to the user, this mechanism is trigged) |
| 2.3 Access to the external carrier                                                 |
| 2.4 Addressing to the object on the carrier                                       |
| 2.5 Comparison of confidentiality markers for the user and resource (in the information security system from the unauthorized access is realized based on the mandatory principle of the access control) |
| 2.6 Blocking an access to the object                                               |
| 2.7 Checking of of the user's access powers (in the information security system from the unauthorized access it is realized on the basis of the access control discretion principle) |
| 2.8 Converting information on the carrier by encryption (in the information security system from the unauthorized access the gamma method is used) |
Table 2. Initialization of the user's rights to work in the system and access to the file catalogue.

| Functions performed by the information security system from the unauthorized access |
|---|
| 2.9 Access of the subject to the secured object |

Figure 2. Initialization of the user's rights to work in the system and access to the file catalogue.

The following model subsystem of the information security system from the unauthorized access describes the user's work with individual objects (figure 3), it is based on the principle of access demarcating by the user's authenticating and limiting its access rights to individual objects of the system. If it is forbidden for the user to work with individual object, then the individual security system from the unauthorized access blocks an access to the object and records this fact in the event log. It helps to identify the facts of the user's unauthorized access to the objects to which they do not have access. This functionality is the malware for simulating the reaction of the information security system from the unauthorized access to actions of the attacker. At peak r29 there is transition to the subsystem "User's work with applied software products", which simulates the user's work with individual software products.

Table 3. User's work with files and programs.

| Functions performed by the information security system from the unauthorized access |
|---|
| 2.9 Subject's access to the secured object |
| 3.1 Request to convert an object |
| 3.2 Block of the object conversion |
| 3.3 Registration of malfunctions with the information security system from the unauthorized access |
| 3.4 Recalculation of file integrity parameters |
| 3.5 Deletion request |
| 3.6 Deletion blocking |
| 3.7 Transformation of the object before deletion |
| 3.8 Object deletion |
| 3.9 Completion of work with the object |
The model subsystem "User's work with applied software programs" (figure 4) includes the most popular software. This subsystem interacts with the subsystem "User's work with files and programs", the connecting peak between is r411. It should be noted that in the model we consider the work only with one software program, without the ability to use other programs in parallel. This system reflects the user's work with a typical software composition, in particular with such as Microsoft Office, ABBY FineReader, Nero, WinRar, TotalCommander.

The model "Destructive impact on the information security system from the unauthorized access" (figure 5) describes the attacker's actions on implementation of the malware through the system data accumulated by him. The preliminary scenario of the malicious impact of the attacker on the secured information resource of the automated system is developed on the basis of threat analysis from the security information data bank of the Federal service for the technical and export control of Russia.

The result of this model is made at peak r24 "Initialization of the user's rights to work in the system and access to the file catalogue", which displays the user's work with the external information carrier.

Figure 3. User's work with files and programs.

Figure 4. User's work with files and programs.
Table 4. User’s work with files and programs.

| Functions performed by the information security system from the unauthorized access |
|---------------------------------------------------------------|
| 4. Start of work with programs                               |
| 4.1 Work with documents                                      |
| 4.2 Work with individual software                            |
| 4.3 Work with browser and in net (local/ global)              |
| 4.4 Use of various servers online                            |
| 4.5 Work with software Microsoft Office                      |
| 4.6 Work with software ABBY Fine Reader                      |
| 4.7 Work with software Nero                                  |
| 4.8 Work with software WinRAR                                 |
| 4.9 Work with software Total Commander                       |
| 4.10 Work with software Lock                                 |
| 4.11 Data or actions from the work with individual objects (files/ folders) |

Figure 5. Destructive impact on the information security system from the unauthorized access.

Table 5. Destructive impacts on the information security systems from the unauthorized access.

| Destructive impact of the attacker on the information resource of the automated system (preliminary scenario) |
|---------------------------------------------------------------------------------------------------------------|
| 5 Actions of the attacker                                                                                   |
| 5.1 Document creation                                                                                       |
| 5.2 Creation of malware in the document as a launch macros jointly with opening of the document             |
| 5.3 Replacement of the "net" document on the carrier into the malware                                       |
| 5.4 Creation of the malware with auto-start function                                                        |
| 5.5 Record of the malware or malicious program on the carrier                                               |
After all performed operations there is the working model of the information security system from the unauthorized access. It allows visualizing what happens at its work on the system level and also take into account the alleged actions of the attacker. The imitation model will be discrete, dynamic, stochastic by the reason that these properties are typical for the information security system from the unauthorized access in the automated system, therefore this model is to be discrete-event, therefore reflecting the properties in time. The probable transition from one state to another is instantaneous and depends on the time of staying in the previous state.

3. Imitation model test for adequacy

We are to test the resulting net for adequacy. As an example we are to demonstrate it by the fist subsystem model. For that we make the required number of steps, resulting in the total number of chips in the states "r2" и "r4", "r04" и "r6", "r5" и "r7" and making 50. In positions of "r04" и "r6" 44 and 6 chips are in figure 6, in positions "r5" и "r7" 49 and 1 chip is in figure 7. Then the chips frequency occurrence in the state of "r2", "r6", "r7" Figure 8 will be as follows:

\[
p_{r2} = \frac{6}{50} = 0.12; \quad p_{r6} = \frac{5}{50} = 0.1; \quad p_{r7} = \frac{1}{50} = 0.02.
\]  
(1)

We are to determine the needed number of runs in net for the probable event occurrence with the precision of \( \varepsilon = 0.01 \) and sufficiency \( D = 0.99 \) under the formula:

\[
N = \frac{p(1-p)}{\varepsilon^2} \left[ \phi_0^{-1} \frac{D}{2} \right]^2,
\]  
(2)

where \( \phi_0 \) – Laplace function. Accordingly the required number of runs "r2", "r6", "r7", for these states will be the following:

\[
N_{r2} = \frac{0.12(1-0.12)}{0.01^2} \approx 7029.1584; \quad N_{r6} = \frac{0.1(1-0.1)}{0.01^2} \approx 5990.76;
\]
\[
N_{r7} = \frac{0.02(1-0.02)}{0.01^2} \approx 1034.6544.
\]  
(3)

Figure 6. The model run to determine the number of chips in the states of "r2" and "r4".
Figure 7. The model run to determine the number of chips in the states of "r04" and "r6".

Figure 8. The model run to determine the number of chips in the states of "r5" and "r7".

Figure 9. Imitation model of subsystem "Login" of the information security system from the unauthorized access with the required number of runs.
Table 6. Summary table of calculated required number of runs for the imitation model of the imitation security system from the unauthorized access.

| Starting peak | End peak | Number of chips | Frequency | N       |
|---------------|----------|-----------------|-----------|---------|
| **Subsystem "PC enabling and user's identification"** |
| r3            | r2       | 6               | 0.12      | 7029.1584 |
| r3            | r4       | 44              | 0.88      | 7029.1584 |
| r5            | r6       | 5               | 0.1       | 5990.76  |
| r5            | r8       | 45              | 0.9       | 5990.76  |
| r6            | r7       | 1               | 0.02      | 1304.6544 |
| r6            | r5       | 49              | 0.98      | 1304.6544 |
| **Subsystem "Initialization of the user's rights to work in the system and access to the file catalogue"** |
| r18           | r21      | 24              | 0.48      | 16614.3744 |
| r18           | r24      | 26              | 0.52      | 16614.3744 |
| r21           | r22      | 49              | 0.98      | 1304.6544 |
| r21           | r23      | 1               | 0.02      | 1304.6544 |
| r22           | r23      | 2               | 0.04      | 2556.0576 |
| r22           | r26      | 48              | 0.96      | 2556.0576 |
| r25           | r26      | 47              | 0.94      | 3754.2096 |
| r25           | r27      | 3               | 0.06      | 3754.2096 |
| r27           | r28      | 23              | 0.46      | 16534.4976 |
| r27           | r29      | 27              | 0.54      | 16534.4976 |
| **Subsystem "User's work with files and programs"** |
| r29           | r31      | 47              | 0.94      | 3754.2096 |
| r29           | r35      | 3               | 0.06      | 3754.2096 |
| r35           | r36      | 48              | 0.96      | 2556.0576 |
| r35           | r37      | 2               | 0.04      | 2556.0576 |
| r36           | r33      | 36              | 0.72      | 13419.3024 |
| r36           | r39      | 14              | 0.28      | 13419.3024 |
| r31           | r32      | 46              | 0.92      | 4899.1104 |
| r31           | r34      | 4               | 0.08      | 4899.1104 |
| **Subsystem "User's work with applied software programs"** |
| r40           | r41      | 15              | 0.3       | 13978.44 |
| r40           | r42      | 17              | 0.34      | 14936.9616 |
| r40           | r43      | 18              | 0.36      | 15336.3456 |
| r42           | r45      | 6               | 0.12      | 7029.1584 |
| r42           | r46      | 8               | 0.16      | 8946.2016 |
| r42           | r47      | 10              | 0.2       | 10650.24 |
| r42           | r48      | 14              | 0.28      | 13419.3024 |
| r42           | r49      | 12              | 0.24      | 12141.2736 |
| **Subsystem "Destructive impact on the information security system from the unauthorized access"** |
| r42           | r51      | 26              | 0.52      | 16614.3744 |
| r42           | r54      | 24              | 0.48      | 16614.3744 |

4. Conclusion
This article discloses the simulation model of the information security system from the unauthorized access. There are its key subsystems and functional components according to the technical documentation [1, 2]. By means of "Hierarchy" tools in CPN Tools the interactions between subsystems are realized, which allows the model to correspond to the really used information security system from the unauthorized access on the information objects. The developed simulation model for the functioning of the information security system from the unauthorized access in the software
environment CPN Tools unlike the current formal models [3] provides the probability-temporal characteristics (as the times to perform security functions). It makes possible to conduct the computational experiment on research of the probabilistic - temporal characteristics of these systems, which are to be used further at the qualitative evaluation of the software efficiency and the information security systems in the automated system on information objects. The developed imitation model of the information security system from the unauthorized access in the software environment CPN Tools in further researches is planned to be used as the basis for analysis and to create the model of counteracting different types of threats from the information security system to secured automated systems.

5. References
[1] Information security system "Guide NT". Administrator's guide. URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (Reference date: 25.08.2019)
[2] Information security system from the unauthorized access "Guide NT". Applied description. URL: http://www.rubinteht.ru/public/opis30.pdf (Reference date: 25.08.2019)
[3] Popov A D 2018 Models and algorithms to access efficiency of the information security systems from the unauthorized access in terms of the temporal characteristics in automated systems for the internal affairs authorities (Ph.D. thesis. Voronezh) URL: https://вн.мвд.рф/Nauka/Dissovetiy/sostojavshiesja_zashhiti_dissertacij
[4] Ventzel E S 1969 Probability theory (Moscow: Science) p 576 (in Russian)
[5] Jensen K, Kristensen L M 2009 Coloured Petri Nets Modeling and Validation of Concurrent Systems (Berlin: Springer-Verlag) p 382
[6] Sinegubov S.V. 2016 Modeling of nets and telecommunication networks (Voronezh: VI MIA RF) p 336 (in Russian)
[7] Zaitsev D A, Shmeleva T R 2006 Simulating Telecommunication Systems with CPN Tools (Students’ book. – Odessa: ONAT) p 60
[8] Grigoryev V A, Karpov A V 2005 Simulation model of the information security system // Software products and systems (Tver: MNIIPY and NII "Centerprogramsystem" №2) pp 26-30 (in Russian)
[9] Peterson D J 1984 Theory of Petri nets and simulation of systems: Translated from English (Moscow: Mir) p 264
[10] Kotov V E 1984 Petri nets (Moscow: Science. Main edition of the physic - mathematical literature) p 160 (in Russian)
[11] Popov A D [et. al.] 2017 Methods to research the probabilistic-temporal characteristics for realizing network attacks in the software environment of the imitation modeling (Bulletin of the Dagestan state technical university. Technical sciences. № 4.) pp 99-113 (in Russian)
[12] Meedeniya D. A. Indika Perera 2013 Model based software design: Tool support for scripting in immersive environments. IEEE 8th International Conference on Industrial and Information Systems pp 248-253
[13] Lukaszewski R, Winiecki W 2006 Petri Nets in Measuring Systems Design. IEEE Instrumentation and Measurement Technology Conference Proceedings, pp. 1564-1569.
[14] Gehlot V, Nigro C 2010 An introduction to systems modeling and simulation with Colored Petri Nets pp 104-118
[15] Shang Guan Wei [et. al.] 2009 Research of System Modeling and Verification Method Combine with UML Formalization Analysis and Colored Petri Net. Third International Symposium on Intelligent Information Technology Application pp 488-491