each functional conversion is performed. In addition, the cited work gives an example of modeling the cryptographic system R_1, the basis of the formalization of which is the Chinese theorem about the remnants. In this case, the following expression was obtained to analyze the time of the R_1 system:

$$Wk_E^{(R_1)}(s) = e^{\left(\beta s + 0{,}5k_1 D s^2\right)}, \quad \beta = k_1 + \left[\left(k_1+1\right)t_{цд} + \left(k_2{}^2+1\right)t_{ум} + \left(k_3-1\right)t_{сл}\right]; \qquad (3)$$

k_i is the number of integer division, multiplication, and addition operations, respectively, normalized for τ (τ=10 for example); t_{idiv} is the time it takes for integer division operations; t_{mul} is the time it takes for multiplication operations; t_{sum} is the time it takes for addition operations.

We shall use (3) to find the equivalent *W*-function of the source code verification process for cryptographic and other ways to protect the data. For the cases set in Table 2 (case 1–q_1=0.1, q_2=0.4, q_3=0.4, case 2–q_1=0.3, q_2=0.1, q_3=0.5. For both cases, D_N=9, k_1=k_2=k_3=2), we shall obtain the *W*-function of R_1 conversion time:

$$Wk_E^{(R_1)}(s) = e^{\left(1.376s + 16.9s^2\right)}. \qquad (4)$$

Then the equivalent *W*-function of the time of the process of testing a cryptographically converted software product

$$Wk_E(s) = \frac{q_1 q_2 q_3 e^{5.04s+67.6s^2}}{1-(p_1+p_2)\mathrm{e}^{1.38s+16.9s^2} + p_1 p_2\,\mathrm{e}^{2.76s+33.8s^2} - q_1 q_2 p_3\,\mathrm{e}^{4.14s+50.7s^2}}, \qquad (5)$$

References

1. Семенов С.Г., Сур О.О Математична модель системи криптографічного захисту електронних повідомлень на основі GERT-мережі Системи управління, навігації та зв'язку»: К.:ЦНДІ навігації і управління, 2012. Вип. 1(21), том 1. С.131-137.

2. Garg Vishal (2014) "Approaches, tools and techniques for security testing" https://www.3pillarglobal.com/insights/approaches-tools-techniques-for-security-testing

TESTING PROCESS MATHEMATICAL MODEL FOR PENETRATION INTO COMPUTER SYSTEMS

Cao Weiling
Department of IT information Centre Neijiang Normal University, Neijiang, China
Chernykh O.
National Technical University «KhPI», Kharkiv, Ukraine

Penetration testing services have become increasingly popular in the IT-industry. A number of popular articles [1] set out in some detail the possible approaches and steps that accompany these services. However, these works vast majority consider this cybersecurity assessment type from a view practical point, based on the expertise in various computer and information infrastructures experience. This, in turn, leads to spectrum and increased run time either unreasonable expansion, without ensuring the appropriate assessment quality, or

possible vulnerabilities and security risks insufficient consideration. The mathematical models' development and research governing penetration testing procedures can optimize these processes (increase their efficiency and IT-infrastructures security).

To solve the problem of the testing process for penetration into computer systems mathematical formalization, we use the GERT-structures graph approach. As arguments for the expediency of such an approach and the mathematical modeling obtained results adequacy, many authors [3, 4] cite the developed methods for building GERT-networks and proven methods for complex GERT-structures preliminary regularization studies results. Simulation results given in works [2] indicate their validity.

The GERT-network interpreting the generalized penetration test algorithm is shown in Fig. 1.

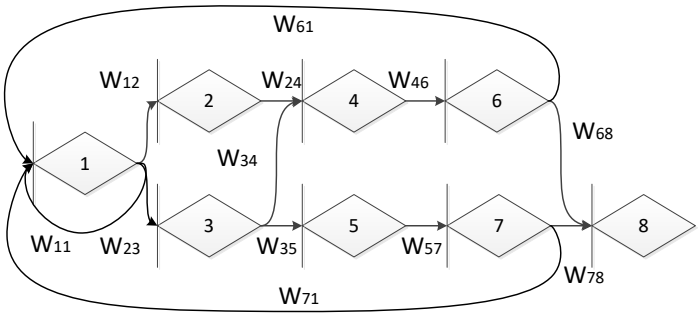

Fig. 1. GERT-network interpreting the generalized testing algorithm diagram

The process under consideration peculiarity lies in the analyzed and processed data heterogeneity. At the same time, organizing feedback various cases are possible. In Figure 1, these cycles are recorded as transitions W_{11}, $W_{12} \to W_{24} \to W_{46} \to W_{61}$, $W_{13} \to W_{34} \to W_{46} \to W_{61}$, $W_{13} \to W_{35} \to W_{57} \to W_{71}$.

However, using the Erlang distribution as the base when formalizing the moment-generating function, will take into account this heterogeneity. By changing the coefficients Q and k positive simulation results can be achieved. Initially, such changes must be made empirically.

References

1. Michael Felderer, Matthias Büchler, Martin Johns, Achim D. Brucker, Ruth Breu, Alexander Pretschner (2016)"Security Testing: A Survey" Advances in Computers Volume 101, pp. 1-51. DOI doi:10.1016/bs.adcom.2015.11.003

2. Semenov, S.G. (2014) "Protection Data in computerized Governors systems", LAP Lambert Academic Publishing GmbH & Co. KG (Saarbrücken, Germany), 2014, 236 p.