Formalization of Cyber Resilience Assessment of Critical Infrastructure Facilities to Phishing Attacks Based on a Set-Theoretic Approach

UDC 004.056

Oleksandr Korchenko[1], Yuliia Khokhlachova[2], Serhiy Skvortsov[3]

State University of Telecommunications, Kyiv, Ukraine,
National University "Kyiv Aviation Institute",
[1]agkorchenko@gmail.com, [2]yuliiahohlachova@gmail.com, [3]ssamailer@gmail.com

In the context of rapid digitalization of critical infrastructure objects, their functioning increasingly depends on complex information and telecommunication systems, which significantly increases the level of cyber risks. One of the most widespread and at the same time effective threats remains phishing attacks, which are based on social engineering methods and aimed at obtaining confidential user information. For critical infrastructure objects, such attacks can lead to serious consequences, including disruption of technological processes, loss of access to critical resources, and cascading failures.

Phishing is a complex multi-level threat that combines technical mechanisms and behavioral aspects. The main target of such attacks is the user, which makes the human factor a key element in the cybersecurity system. Even with modern information security tools in place, human errors are most often the cause of successful attacks.

Traditional cybersecurity approaches based on prevention and detection of incidents prove to be insufficient in the modern threat environment. In this regard, the concept of cyber resilience becomes relevant, which implies the ability of a system not only to resist attacks but also to maintain critical functions during an incident, quickly recover after it, and adapt to new operating conditions.

The purpose of the study is to formalize the process of assessing the cyber resilience of critical infrastructure objects under phishing attacks based on a set-theoretic data model. The proposed approach allows the transition from qualitative analysis to quantitative evaluation of the effectiveness of cybersecurity measures.

In the proposed model, phishing is considered as an element of the set of cyber threats that affects authentication mechanisms and user behavior. A hierarchical structure is introduced, which includes sets of strategic goals, tasks, subtasks, and basic cyber resilience measures. Each element of this structure is assigned a unique identifier, which ensures a formalized mapping between threats and countermeasures.

Strategic goals of cyber resilience include anticipation, withstanding, recovery, and adaptation. To achieve these goals, a set of tasks and subtasks is defined, which are implemented through basic measures. Such decomposition allows a detailed analysis of the contribution of each element to the overall level of cyber resilience.

In the case of phishing attacks, key measures include the implementation of multi-factor authentication, systematic personnel training, the use of analytical monitoring and anomaly detection tools, restriction of user privileges, and segmentation of access to resources. Additionally, it is important to implement security policies that regulate user behavior.

The proposed model allows formalizing the contribution of each measure to cyber resilience through the use of functional dependencies. This makes it possible to determine optimal combinations of measures depending on the type of threat and system characteristics.

A key element of the model is the introduction of quantitative evaluation metrics, including detection time, response time, level of functionality preservation, and the degree of impact on critical processes. In the context of phishing attacks, it is important to determine the interval between credential compromise and its detection, as well as the effectiveness of incident localization measures.

The model also allows analyzing different response scenarios and evaluating their effectiveness. This creates a basis for making informed management decisions and optimizing resources.

The use of the set-theoretic approach ensures flexibility and scalability of the model. It can be adapted to various types of critical infrastructure objects and allows integrating new threats without changing the basic structure.

The practical significance lies in the possibility of using the model to improve cybersecurity effectiveness, optimize costs, and ensure stable system operation.

Thus, the proposed approach provides a systematic assessment of cyber resilience, enables the transition to quantitative analysis, and increases the effectiveness of countering phishing attacks.

Prospects for further research include expanding the model to other types of attacks, integration with decision support systems, and the development of software tools for automated cyber resilience assessment.

1. Bodeau D, Graubart R, McQuaid R, Woodill J. Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods. (The MITRE Corporation, Bedford, MA), MITRE Technical Report 2018.
2. Bodeau, D., & Graubart, R. Cyber Resiliency Engineering Framework. MITRE Corporation Technical Report MTR110237 2011.
3. Bodeau, D., Brtis, J., Graubart, R., & Salwen, J. Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques. MITRE Technical Report MTR150264 2015.
4. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160 2021, Vol. 2, Rev. 1.