UDC 004.056.53:004.415:004.89:621.39 **doi: 10.26906/SUNZ.2025.4.207-213**

Ievgen Samborskyi[1], Heorhii Krykhovetskyi[2]

[1] State University "Kyiv Aviation Institute", Kyiv, Ukraine
[2] Defence Intelligence Research Institute, Kyiv, Ukraine

SYNTHESIS OF THE DIGITAL TWIN OF THE LOGICAL-DYNAMIC INFORMATION AND EVENTS MANAGEMENT SYSTEM FOR THE SECURITY OF COMPUTER SYSTEMS OF THE MOBILE CELLULAR INFORMATION AND COMMUNICATION NETWORK

Abstract. The article focuses on the aspect of information security and notes that currently the modern mobile information and communication cellular network is one of the most vulnerable and at the same time important objects of the critical information infrastructure of the state. It serves a wide range of users who make decisions for the organization of public administration, and also provides digital communication to a number of other important systems from the population to departmental structures. That is why this network acts as a priority object in the context of organizing effective management of its information security events. To organize the reliable functioning of this important object, a new approach to the synthesis of a digital twin of the information and security event management system of computer systems of the cellular mobile information and communication network is proposed. The proposed synthesis is based on a logical-dynamic approach to modeling security events in modern computer systems, attack scenarios and mechanisms for responding to these information security incidents by forming appropriate effective control influences. The architecture of the digital twin, the algorithm for its synthesis are considered, and possible approaches for implementing the integration of this virtual object with such platforms as Wazuh, Streamlit, Neo4j, AWS IoT are proposed. Verification and testing are carried out using the example of a DDoS scenario, and the results of the synthesis algorithm implementation are presented. The effectiveness of the model in detecting threats and adapting to intensive changes in the security environment of the computer system of the mobile digital network is shown.

Keywords: digital twin, management system, information security, security event, synthesis, logical-dynamic model, security event management, mobile network, integration, SIEM, Wazuh.

Statement of the problem

In the current conditions of information confrontation and hybrid aggression, digital cellular communication currently plays a key role in the functioning of critical information infrastructure facilities of the state, including energy, the financial system, logistics, state registers, and especially corporate secure communications. Ensuring the security of computer systems, which are the core of the mobile information and communication network system, has become extremely relevant due to the increase in the number and complexity of threats to the information security of these controlling computing facilities.

A vivid example of these threats is a large-scale cyberattack on one of the largest mobile operators in our country - "Kyivstar" in December 2023. This attack led to a long and serious disruption of digital communications, disruptions in the work of banking, logistics, energy and administrative services. This incident, in addition to organizational problems in the management of this digital cellular structure, revealed both the technical and conceptual inability of traditional information and security event management systems, which are currently operated in the information and communication network system, to effectively and reliably resist complex multi-level information security incidents in real time.

Organizing effective information and security event management in the conditions of dynamic, heterogeneous and distributed mobile cellular digital networks requires the urgent implementation of significantly new approaches. Methods that allow synthesizing adaptive, attack-resistant solutions with a high level of efficiency in information and security event management deserve special attention. In this context, an important The concept of digital twins plays a role, which allows you to synthesize virtual models of PCM objects and display them in real time. As a rule, the concept of digital twins synthesis is based on modern technologies, namely: Industry 4.0 technologies. At the same time, it is imperative to take into account that mobile information and communication network system is one of the most vulnerable and at the same time critically important super-complex objects of the critical information infrastructure. It serves a very wide range of users and systems – from the population to state departmental structures. That is why information and communication network system acts as a priority object of information security event management. Therefore, an urgent scientific and applied task of synthesizing digital twins of logical-dynamic information management systems and security events of the information and communication network system arose and is emerging, which requires the development of new models, methods and algorithms to increase the level of security, interference and functional stability of these digital means.

Analysis of recent research and publications

In recent years, there has been a sharp increase in scientific interest in the concept of creating and improving digital twin technologies as an effective tool for improving the security of information and communication networks. In the field of information and security event management of a computer system, digital twins allow creating virtual copies of critical

information infrastructure objects capable of monitoring, analyzing states, and modeling the development of security events in real time. Let us analyze the latest research presented in a number of fundamental publications. It should be noted that the scientific work [1] is decisive for the synthesis of logical-dynamic models of the digital twin of the information and security event management system of a computer system which confirms the relevance of this approach for complex information systems. In articles [2–3], the authors substantiate the feasibility of using a logical-dynamic approach in computer system security tasks with a high degree of criticality, demonstrating its adaptability, scalability, and compliance with the dynamic nature of events in cyberspace.

Particular attention is paid to the problem of detecting attacks such as APT, MITM, DDoS in mobile networks, which have a high dynamic topology and limited depth of response from classical SIEM/SOAR platforms. In this context, a digital twin with a built-in logical-dynamic model is able not only to reproduce the architecture of the information and communication network, but also to model the consequences of security events, predict critical states and launch control actions. A systematic approach to the synthesis of such models is disclosed in the works [4–7]. They propose algorithmic mechanisms for distributing response efforts based on models of radio-electronic influence and logical-event schemes for organizing control processes.

The conducted analysis of scientific sources indicates the relevance and existing powerful potential of the logical-dynamic approach for the tasks of algorithmization of the digital twin of the information and security event management system in distributed critical environments – the information and communication network. Information and security event management systems of the computer system of the information and communication network with a digital twin, in which this approach is implemented, have significant advantages over classical SIEM/SOAR systems due to the possibility of adaptive response to security events, forecasting the development of information security incidents, modeling the mutual correlation of security events in information and communication networks as well as the operational and effective formation of security event management in information and communication networks. This determines the scientific novelty and practical value of further research on the synthesis of a digital twin with a logical-dynamic core in the computer system of mobile cellular information and communication networks.

The purpose of this work is to substantiate and develop an effective approach to the synthesis of digital twins of the logical-dynamic information and event management system of the computer system of the mobile cellular information and communication network as a critical object of the national information infrastructure. It is advisable to focus particular attention on the construction of a synergized architecture of the digital twin, the creation of an algorithm for its synthesis based on the logical-dynamic model, as well as the integration of the digital twin with modern platforms for monitoring and processing security events, such as Wazuh, Streamlit, Neo4j, AWS IoT, etc. Along with this, the goal is also to demonstrate the effectiveness of the proposed model in conditions of DDoS scenarios and highly dynamic processes in the computer system of the information and communication network. This will allow to ensure a high level of security and functional stability of the computer system, to predict the development of possible threats (especially “zero-day”), to automatically form response strategies and adaptively manage security events and a number of other risks in critical conditions. Therefore, the main goal of the article is to propose new and effective approaches to the synthesis of digital twins of logical-dynamic information and event management systems that provide reliable protection of the computer system from modern existing threats, as well as from zero-day threats.

Presentation of the main material

To develop fundamentally new and effective methods for synthesizing a digital twin of logical-dynamic information management systems and security events that provide reliable protection of the computer system of the information and communication network from a wide range of existing threats to their security, and, especially, from zero-day threats we take into account that this network is the most vulnerable among all state objects of critical information infrastructure.

Among the key types of possible information threats that are generators of computer system security events we should especially note the following:

– traffic interception (man-in-the-middle);

– jamming (suppression) of digital communication radio channels;

– attacks related to malicious software (malware), including zero-day;

– internal threats to the computer system;

– APT attacks with a phased impact on the infrastructure of the information and communication network.

The specified security events are characterized by high dynamics, ambiguity and interdependence which makes it impossible to effectively process them by traditional means. In this regard, the task of formalizing the process of managing the security events of the information and communication network as a logical-dynamic system arises in order to integrate it into the structure of the information and security event management system of the digital twin. It should be noted that the mobile cellular information and communication network has a number of specific characteristics that significantly affect the requirements for the synthesis of the digital twin. Let us consider them in more detail:

– dynamic topology: network nodes (base stations, routers, switches, etc.) constantly and dynamically change their location and load depending on the structural geography of a significant number of users.

– heterogeneity of devices: different types of terminals, protocols, standards (4G, 5G, LTE).

– high traffic density: especially in highly urbanized areas which significantly complicates monitoring and rapid response to computer system security events.

– criticality of services: servicing emergency and special services, medical facilities, energy and logistics facilities.

The above features require the digital twin of the information and event management system for the security of the computer system of the information and communication network to have the ability to adaptively model, quickly respond to changes in parameters, and integrate with the information and event management systems for the security of the computer system available in the network.

To detail the wide range of requirements for the digital twin, we propose a formalized model:

$$DT = (F, T, A, O), \quad (1)$$

where F – functional requirements; T – technical requirements; A – analytical requirements; O – organizational requirements.

Each of these elements of the proposed synthesized model (1) is detailed in the form of subsets, namely:

$$F = (f_1, f_2, ..., f_n);\ T = (t_1, t_2, ..., t_n);$$
$$A = (a_1, a_2, ..., a_n);\ O = (o_1, o_2, ..., o_n).$$

The implementation of effective security event management processes for a computer system of a mobile cellular information and communication network requires that the digital twin of the security information and event management system meet a number of requirements covering functional, technical, analytical and organizational aspects. Its architecture must be flexible, scalable, secure and fully comply with international security standards. Let us define these requirements, which will become the basis for building an effective logical-dynamic security information and event management system using a digital twin. At the same time, this virtual object must provide the implementation of the necessary functions, namely:

– monitoring of current and previous security events;

– reconstruction of security event chains and their destructive effects on the processes of functioning of the computer system of the information and communication network;

– forecasting the state of the information and communication network in response to all possible incidents of information security of the computer system;

– generation of management actions for prompt and effective counteraction to threats to the computer system of the information and communication network.

At the same time, the requirements for the digital twin of the information and event management system for the security of a computer system of a mobile information and communication network include the following:

– the ability to integrate with telemetry, logs, NetFlow, syslog;

– display of the current state of the topology of the information and communication network and all its component segments;

– formalization of system behavior in the form of a logical-dynamic model;

– prediction of the consequences of security events and the prompt formation of management responses to incidents;

– compatibility with real security platforms for information and communication networks such as SIEM/SOAR.

The above indicates that the synthesis of digital twins of the information and event management system of a computer system of an information and communication network with a logical-dynamic core is a complex but critically necessary scientific task that includes architecture design, state formalization, transition modeling, and integration with information and management platforms of digital networks.

We synthesize the functional architecture of the digital twin of the information and security event management system of the computer system of the information and communication network. In the process of synthesis, we take into account that this algorithmic and software tool is a virtual analogue of the physical system, which provides real-time monitoring, analysis, forecasting and management of security events. The architecture of such a twin should be based on a logical-dynamic approach, which provides modeling of discrete states of the system and their transitions under the influence of external and internal security events.

The synthesized structure of this virtual analogue of the physical system - the information and security event management system of the computer system of the information and communication network consists of the following synergized modular subsystems, namely:

– information and communication network structure module – a virtual model of the topology of a mobile cellular information and communication network. It includes nodes, channels, base stations, switches, routers. It is implemented through Neo4j – a graph database and is constantly updated in real time based on information from the API *(Application Programming Interface)* and telemetry about the network status.

– data module (data aggregation level module) – aggregates data from information and communication network telemetry, log files, network security events, SNMP queries, NetFlow, syslog. Provides normalization, time synchronization and data processing. Works with Kafka, Fluentd or OpenTelemetry.

– logical-dynamic modeling module (*logical-dynamic core*) – implements a logical-dynamic model in the form of a tuple $LDM = (S, E, M, T)$, where S – a set of system states – an information and communication network; E – multiple security events; M – computer system status monitoring functions, T – rules for transitions between states of a computer system. This module allows you to formalize the behavior of this computing and control system and identify its critical states, taking into account (1).

– visualization and interpretation module – an interactive interface for displaying the current state of the system, forecasting results, and recommendations for prompt response through the formation and implementation of control actions. Implemented using Streamlit, Grafana, Kibana.

– SIEM/SOAR integration interface – exchange of events, notifications and control commands with systems such as Wazuh, Splunk, TheHive, OpenCTI. Provides two-way exchange with SOC analytics.

– response orchestrator – an event response automation subsystem that supports playbook scenarios implemented in the form of logical trees. These logical trees are activated by a digital twin depending on the threat vector model for the computer system of the information and communication network.

The interaction between the components is implemented via a data bus with support for the publish–subscribe model. This allows you to dynamically update the model, adapt it to changes in the states of the information and communication network and provide a cyclic mechanism in security event processing algorithms, namely: *"Security event → Analysis → Forecast → Management decision → Response → Feedback"*.

The synthesized architecture of the digital twin is a system for managing information and security events of a computer system of an information and communication network, built on the basis of a logical-dynamic approach, presented in Fig. 1.

The developed algorithm for synthesizing a digital twin consists of a number of synergized sequential stages. Each of them involves the gradual formalization, modeling and integration of a logical-dynamic approach in the synthesized architecture (Fig. 1) of the digital model. The main goal of the proposed synthesis is to build a digital twin capable of independent analysis of security events, predicting their consequences, and, especially, optimizing decision-making support in the security environment of a mobile cellular information and communication network. The synthesis algorithm includes the following step-by-step stages:

Stage 1. Identification of the modeling object:

– identification of the components of the information and communication network as an object of critical information infrastructure;

– identification of key control points of security events, information flows and typical information security incidents.

Stage 2. Formalization of events and states:

– construction of a set of discrete states (for example: "normal", "threat detected", "response activated");

– definition of a set of events (incidents, anomalies, intrusions, etc.);

– construction of monitoring functions that determine under what conditions a certain security event is recorded;

– formalization of rules for transitions between states under the influence of security events (in the form of logical rules or graphs).

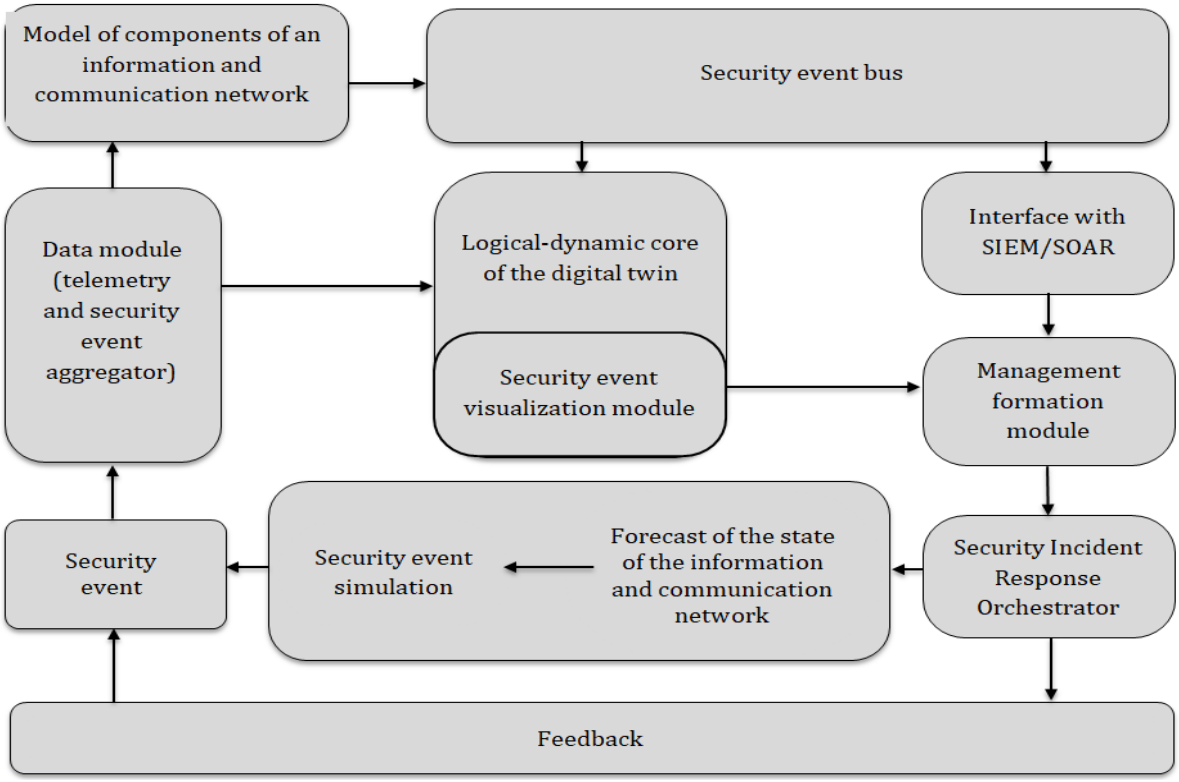

Fig. 1. Architecture of the digital twin of the information and event management system of the security control computer system of the information and communication network, built on a logical-dynamic approach

Stage 3. Construction of a logical-dynamic model:

– combining sets into a tuple $LD = (S, E, M, T)$;

– checking the model for conflicts, completeness, and the absence of cycles without a solution;

– modeling typical scenarios of information security incidents and checking the model's response to these events.

Stage 4. Integration with the digital infrastructure of the information and communication network:

– implementation of communication with telemetry sources (log files, network events, SNMP);

– construction of adapters for visualization, response orchestration, interaction with SOC.

Stage 5. Automation and training of the digital twin:

– implementation of mechanisms for adapting the model to new security events, and especially zero-day;

– application of machine learning methods to detect new event scenarios;

– training of transition rules based on statistical data on security events (formation of a reflexive model).

Analysis of the synthesized digital twin algorithm shows that its implementation in real systems for managing information and security events of a computer system of an information and communication network will allow us to gradually move from a description of an object to a functional model with predictive, reactive and adaptive capabilities for organizing security event management, which can be flexibly integrated into modern complex protection systems for these critically important digital networks.

Let us verify and validate the synthesized digital twin. It should be noted that after building this virtual digital tool for the information and security event management system of a computer system of an information and communication network, its verification and validation are critically important stages. These processes allow us to assess the correct functioning of the model, its compliance with the expected characteristics as well as the ability to detect and respond to all possible security events in a mobile network. Let us take into account that verification involves an internal comprehensive check of the logic of the model and its components, namely:

– checking the correctness of the definition of sets of states *S*, events *E* and transition rules *T*;

– the absence of logical conflicts, ambiguous transitions or looping of models;

– the conformity of the model to the given architecture and structure of the digital twin.

Validation is aimed at checking the model in real or close to real conditions of the functioning of a real information and communication network.

It involves:

– testing the behavior of the digital twin based on attack scenarios (for example, DoS, APT, MITM);

– comparing the model's response with reference response scenarios in a real SIEM – information and communication network system;

– determining the accuracy, completeness and timeliness of incident detection.

The validation scenario algorithm involves the following sequence of actions:

1. An "abnormal communication channel overload" event is generated.
2. The model records a change in metrics through a telemetry aggregator.
3. The logical-dynamic model enters the "threat detected" state.
4. The orchestrator's response scenario is activated to block traffic.
5. The result is saved and displayed in the visualization interface.

The verification performed ensures the structural consistency of the digital twin, and the validation results indicate its effectiveness in the context of compensating for the destructive consequences for the computer system of the information and communication network in the event of real threats to its security. Synergization of verification and validation allows to increase the confidence in the model and ensure its practical suitability for the implementation of integration processes in the real environment - modern mobile cellular information and communication networks (Table 1).

Table 1 – **Integration of the digital twin with the real information and communication network environment**

Component / platform	Task / role	Integration features	Example of implementation
Wazuh (SIEM)	Monitoring security events and logs of information and communication network nodes	Using agents, triggers, REST API; connecting to Wazuh manager	Detection of DoS, MITM, incidents in base stations of the information and communication network
Streamlit	Interactive visualization of model states	Web interface; display of states, graphs, what-if modeling	Real-time model state transition graph
AWS IoT Core	Telemetry collection, connecting devices to the information and communication network	MQTT, Lambda functions, Amazon Timestream for analyzing and storing security events	Channel congestion analysis, time series storage
Message brokers (Kafka, MQTT)	Real-time transmission of events to a digital twin	Providing publish–subscribe logic, buffering security events	Delivery of telemetric information from information and communication network nodes to the LDM module
Response mechanisms (SOAR/Playbook)	Initiating action in response to a real threat	Support for two-way exchange and implementation of security incident response scenarios	Automatic blocking of traffic in the event of a DoS attack

To confirm the operability of the synthesized digital twin of the information and event management system of the computer system of the information and communication network, an experimental model was implemented in a virtual environment. A conditional DDoS attack on a computer system, which is the control node of the mobile information and communication network was chosen as a test scenario.

The following implementation tool environments were selected [8–10]:

Streamlit – for building a digital twin visualization interface;

Python – implementation of the logical-dynamic kernel and analysis algorithms;

Neo4j – graph database for modeling the structure of the PCM and states;

MQTT – for modeling telemetry streams;

Wazuh – as a source of real logs and security events. During the experiment, the digital twin recorded a suspicious load coming from a certain network segment.

An event “traffic excess anomaly” was generated, which initiated the transition to the “threat detected” state.

The model activated a response scenario: temporary traffic isolation, redirection of logs to SIEM. During testing, the following results of the digital twin’s operation were recorded (Table 2).

Table 2 – **Digital twin testing results during a *DDoS*-scenario**

Parameters	Parameter values	Efficiency assessment	Comments of the experiment
Average threat detection time	up to 3 sec.	High speed	Within target threshold (<5 sec.)
Number of false positives	1 of 20 events	False positives – to 5%	Acceptable level for SIEM class
CPU load	45–60 %	Average load	Peak – when processing complex scenarios
Updating rules during an attack	3 new rules (with automatic update)	Adaptability confirmed	Saved to a graph database – an array of security events

Conclusions

As a result of the research, one of the possible approaches to building digital twins of mobile information and communication networks was implemented, the basis of which is the logical-dynamic modeling of security event management processes.

The synthesized digital event architecture provides structured synergization of information and communication network nodes, security events, computer system states and response scenarios to information security incidents.

The proposed model synthesis algorithm allows for the sequential implementation of key stages of building a digital representation of the system, including the formalization of security events, the construction of logical transitions and integration into real environments of the information and communication network.

Particular attention is paid to practical aspects of integration with security tools, namely: *Wazuh*, *AWS IoT*, *Streamlit*, *Neo4j*.

Testing in a virtual environment of the information and communication network showed the ability of the synthesized digital twin to:

– rapid identification of threats (less than 3 seconds);

– minimizing false positives (≈5%);

– dynamic updating of reaction logic;

– flexible visualization of the current state and “what-if” scenarios.

The results obtained indicate the effectiveness of the logical-dynamic approach to managing security events in a computer system of critical information infrastructure and the feasibility of using a digital twin to increase the level of situational awareness, adaptability and reactivity in the management of critical information and communication infrastructures.

REFERENCES

1. Samborskyi E. I., Peleshok E. V. Synthesis of Logical-Dynamic Information Management Systems and Security Events of Computer Structures. Control, Navigation and Communication Systems. – 2025. – № 2 (72). – P. 185–194. DOI: https://doi.org/10.26906/SUNZ.2025.2.185-194
2. Pavlenko P. M., Samborskyi Ye. I. Upravlinnia informatsiieiu i podiiamy bezpeky kompiuternykh system iz vykorystanniam lohiko-dynamichnykh modelei. Information Technology and Security. 2025. T. 13, № 1 (24). 43–54. DOI: https://doi.org/10.20535/2411-1031.2025.13.1.328764 [in Ukrainian].
3. Sholokhov S. M., Pavlenko P. M., Nikolaienko B. A., Samborsky I. I., Samborsky E. I. The method of optimizing the distribution of radio suppression means and destructive software influence on computer networks. Radio Electronics, Computer Science, Control. – 2023/2024. – № 4 (67). – P. 16–29. DOI: https://doi.org/10.15588/1607-3274-2023-4-2
4. Cherdantseva Y., Burnap P., Blyth A. et al. A review of cyber security risk assessment methods for SCADA systems. Computers & Security. 2016. Vol. 56. P. 1–27. DOI: https://doi.org/10.1016/j.cose.2015.09.009
5. Radanliev P., De Roure D., Nurse J. et al. Digital twins: Concepts and use cases in cyber security risk assessment. Journal of Cyber Security Technology. 2022. Vol. 6(3). P. 147–174. DOI: https://doi.org/10.1080/23742917.2021.1982822

6. Vasyliev V. V., Kovalenko O. S. Intelektualni systemy vyiavlennia zahroz dlia kiberzakhystu krytychnoi infrastruktury. Kiberbezpeka: osvita, nauka, tekhnika. 2023. № 3. S. 42–49. DOI: https://doi.org/10.28925/2663-4023.2023.3.4249 [in Ukrainian].
7. Gamil A. et al. A framework for real-time threat detection and mitigation using digital twins in IoT networks. IEEE Internet of Things Journal. 2021. Vol. 8(12). P. 9740–9752. DOI: https://doi.org/10.1109/JIOT.2020.3046026
8. Wazuh. The Open-Source Security Platform. Documentation. URL: https://documentation.wazuh.com
9. AWS IoT Developer Guide. URL: https://docs.aws.amazon.com/iot
10. Neo4j Graph Data Platform. URL: https://neo4j.com.

Received (Надійшла) 13.08.2025
Accepted for publication (Прийнята до друку) 12.11.2025

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Самборський Євген Іванович – аспірант кафедри організації авіаційних перевезень Державного університету "Київський авіаційний інститут", Київ, Україна;
Ievgen Samborskyi – Postgraduate student, Department of Air Transportation Organization, State University "Kyiv Aviation Institute", Kyiv, Ukraine;
e-mail: seinauedu@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-4441-1947.

Криховецький Георгій Яремович – кандидат технічних наук, старший науковий співробітник, Науково-дослідний інститут воєнної розвідки, Київ, Україна;
Heorhii Krykhovetskyi – Candidate of Technical Sciences (PhD), Senior Researcher, Defence Intelligence Research Institute, Kyiv, Ukraine;
e-mail: kgeorg@ukr.net; ORCID: https://orcid.org/0009-0001-2981-7810;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58697828100&origin=resultslist.

Синтез цифрового двійника логіко-динамічної системи управління інформацією та подіями безпеки комп'ютерних систем мобільної стільникової інформаційно–комунікаційної мережі

Є. І. Самборський, Г. Я. Криховецький

Анотація. У статті акцентовано особливу увагу на аспекті інформаційної безпеки та відмічено, що наразі сучасна мобільна інформаційно-комунікаційна стільникова мережа є одним із найбільш уразливих та водночас важливих об'єктів критичної інформаційної інфраструктури держави. Вона обслуговує широке коло користувачів, які приймають рішення для організації державного управління, а також забезпечує цифровим зв'язком низку інших важливих систем від населення до відомчих структур. Саме тому ця мережа і виступає як пріоритетний об'єкт у контексті організації ефективного управління подіями її інформаційної безпеки. Для організації надійного функціонування цього важливого об'єкта запропоновано новий підхід до синтезу цифрового двійника системи управління інформацією і подіями безпеки комп'ютерних систем стільникової мобільної інформаційно-комунікаційної мережі. В основу запропонованого синтезу покладено логіко-динамічний підхід до моделювання подій безпеки в сучасних комп'ютерних системах, сценаріїв атак та механізмів реагування на ці інциденти інформаційної безпеки за рахунок формування відповідних ефективних управляючих впливів. Розглянуто архітектуру цифрового двійника, алгоритм її синтезу, а також запропоновані можливі підходи для реалізації інтеграції цього віртуального об'єкта з такими платформами як Wazuh, Streamlit, Neo4j, AWS IoT. Проведено верифікацію та тестування на прикладі DDoS-сценарію, наведено результати реалізації алгоритму синтезу. Показано ефективність моделі у виявленні загроз та адаптації до інтенсивних змін безпекового середовища комп'ютерної системи мобільної цифрової мережі.

Ключові слова: цифровий двійник, система управління, інформаційна безпека, подія безпеки, синтез, логіко-динамічна модель, управління подіями безпеки, мобільна мережа, інтеграція, SIEM, Wazuh.